Analysis of Industrial Drivers and Societal Needs:

towards new avenues in EU-US ICT collaboration

Authors: Haydn Thompson, *THHINK – UK*
Daniela Ramos-Hernandez, *THHINK - UK*

ICT Policy, Research and Innovation
for a Smart Society

October 2016

www.picasso-project.eu

PICASSO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 687874.

About the PICASSO Project

The PICASSO project "ICT Policy, Research and Innovation for a Smart Society: towards new avenues in EU-US ICT collaboration" (January 2016 – June 2018), funded under the European Union Horizon 2020 programme, brings together EU and US prominent specialists with the aim of reinforcing EU-US ICT collaboration in pre-competitive research in key enabling technologies related to societal challenges of common interest – 5G Networks, Big Data, Internet of Things and Cyber Physical Systems - and to support the EU-US ICT policy dialogue.

The PICASSO project provides an exchange platform for EU and US experts through three EU-US thematic ICT Expert Groups (5G Networks, Big Data, and IoT/CPS) and one EU-US ICT Policy Expert Group. The synergy between experts in ICT policies and in ICT technologies is a unique feature of PICASSO with benefits to both the policy and the technology communities in the EU and the US. Further, interested EU and US specialists are invited to comment on/contribute to the project analytical materials and to participate in project workshops, information sessions and webinars.

Based on a Panorama Report covering the ICT landscape in the EU and US, as well as an in-depth analysis of industrial drivers and societal needs in the three strategic technology domains 5G Networks, Big Data, and Internet of Things/Cyber Physical Systems, the Expert Groups will develop Opportunity Reports, recommend priorities for EU-US ICT collaboration, and propose measures to stimulate the policy dialogue in these areas. Policy experts will identify policy gaps and prepare Policy Briefs on data protection and privacy, security, standards, spectrum…, as well as an ICT White Paper.

A tool named "CROSSROADS - Your EU-US ICT info-hub" will be made available as a mobile application, but also as a section of the project website, providing extensive support and information on EU-US collaboration opportunities (Horizon 2020 and US ICT programmes) and other relevant information.

The PICASSO consortium is combining academic, industrial and policy support experience and includes the EU-based partners Technische Universität Dortmund and Technische Universität Dresden, Germany, THHINK Wireless Technologies, UK, Athens Technology Centre, Greece, Agenzia per la Promozione delle Ricerca Europea, Italy, GNKS Consult, The Netherlands, and the US-based partners Honeywell International, The Miami-Florida Jean Monnet Center of Excellence (MFJMCE) at Florida International University, and the Technological Leadership Institute, University of Minnesota, USA. The project is supported by NIST – the National Institute of Standards and Technology, USA. The PICASSO partnership is led by inno TSD, France.

More Information and Contact:

s.klessova@inno-group.com project coordinator

www.picasso-project.eu

@picasso_ICT

PICASSO – EU/US ICT research, innovation and policy collaboration

Authors (Organizations):

Haydn Thompson (THHINK)

Daniela Ramos-Hernandez (THHINK)

Inputs from 5G, Big Data, CPS/IoT and Policy Expert Groups

Reviewers (Organization):

Inno, 5G Expert Group, CPS/IoT Expert Group, Big Data Expert Group and Policy Expert Group

Abstract: This public report provides an analysis of EU-US industrial drivers and societal needs/barriers, and highlights initial proposals for collaboration opportunities which will be discussed, refined and prioritised by the Expert Groups in the next stages of PICASSO. As a starting point an analysis was performed of the "Panorama of ICT landscape in EU and US: ICT, Policies, regulations, programmes and networks in the EU and US" deliverable to identify industrial drivers, societal needs and policy gaps and from this extract possible areas for collaboration on research and policy, regulations and standards. Interviews were then performed with key industrial actors from large, mid-cap and SME companies from the EU and US in the Smart Cities, Smart Transportation and Smart Energy sectors. In total 150 key actors were approached for the questionnaire and 70 face-to-face interviews were conducted. The questionnaire was also made available via the PICASSO website. The interviews focused on societal challenges and the application domains, but also including elements related to technological issues, needs, trends and funding needs. Information was also gathered on both industrial drivers and barriers to exploitation, e.g. regulations, lack of standards, lack of business models. This identified 61 potential recommendations covering a broad range, however, some common themes were put forward by different industrial sectors in terms of the needs for standards for interoperability of interconnects, wireless communications, protocols and for data exchange. An overriding message was one of the need for data governance, clarity on data ownership and regulation for privacy and the strong need for security. Overall there is good correlation between the recommendations identified in the analysis of current activities and those highlighted by industry with the most fertile areas being in Smart Transportation and Smart Cities.

Relevant ICT PPPs, ETPs and KIC ICT were also contacted : SmartGrids, ETIPWind, ARTEMIS, ENIAC, EPoSS, euRobotics, NEM, NESSI, Networld 2020, Photonics 21, Manufacture, ACARE, ALICE, ERRAC, ERTRAC and Waterborne, to get their opinions with respect to the questionnaire. The views of the PICASSO Expert Groups were also collected. The report highlights that there are key opportunities in the areas of Smart Cities and IoT/CPS which are rapidly developing areas and where there are common research, regulatory and standardisation needs. There are also great opportunities in the areas of Smart Energy and Smart Transportation, however, here there is existing regulation and legislation which needs to be harmonised. For the underlying technologies, which are the basic building blocks of future applications: 5G, Big Data and IoT/CPS, there are many opportuntiies to work together which would allow bilateral access to EU and US markets and would allow technology and products to be sold on the world stage increasing the competitiveness of EU and US companies in existing and developing markets.

Keywords: Smart Cities, Smart Energy, Smart Transportation, 5G, Big Data, IoT, CPS

Disclaimer

This document is provided with no warranties whatsoever, including any warranty of merchantability, non-infringement, fitness for any particular purpose, or any other warranty with respect to any information, result, proposal, specification or sample contained or referred to herein. Any liability, including liability for infringement of any proprietary rights, regarding the use of this document or any information contained herein is disclaimed. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by or in connection with this document. This document is subject to change without notice. PICASSO has been financed with support from the European Commission. This document reflects only the view of the author(s) and the European Commission cannot be held responsible for any use which may be made of the information contained herein.

Change History

Haydn Thompson 19/10/2016	Draft Circulated
Haydn Thompson 28/10/2016	Issue 1
Haydn Thompson 7/11/2016	Public Version of Report

Table of Contents

1 Executive Summary 11
2 Introduction 13
2.1 Objectives, Scope and Data Gathering Approach of the Deliverable 13
3 Analysis and Key Messages from the Panorama Report D1.3 15
3.1 Smart Cities 16
3.1.1 Smart Cities - Potential Areas for Collaboration 17
3.2 Smart Energy and Smart Grid 17
3.2.1 Smart Energy and Smart Grids - Potential Areas for Collaboration 19
3.3 Smart Transportation 19
3.3.1 Road 20
3.3.2 Rail 21
3.3.3 Air Transportation 22
3.3.4 Marine 22
3.4 5G 23
3.4.1 5G – Potential Areas for Collaboration 24
3.5 Big Data 24
3.5.1 Big Data – Potential Areas for Collaboration 25
3.6 CPS/IoT 25
3.6.1 CPS/IoT – Potential Areas for Collaboration 27
3.7 Conclusions from Analysis of Panorama Report 28
4 Industry Interviews 29
4.1 Overview of Companies Interviewed 31
4.2 Smart Cities 31
4.3 Automotive Sector 32
4.4 Aerospace Sector 34
4.5 Maritime Sector 35
4.6 Rail Sector 35

4.7 Space Sector **36**

4.8 Energy Sector **36**

4.9 Automation Sector **38**

4.10 Diagnostics and Plant Monitoring **40**

4.11 Information Technology Sector **41**

4.12 Wireless/Telecoms Sector **41**

4.13 Software Development and Tools Sector **43**

4.14 Research Organisations and Networks **43**

4.15 Security and Data Protection **44**

4.16 Standardisation **44**

4.17 Recruitment Sector **45**

4.18 Key Messages and Recommendations from Industry **45**

4.20 Summary of Key Recommendations **52**

5 Views of ETPS, PPPs and Key Clusters **54**

5.1 Networld2020/5G PPP **55**

5.2 High Performance Computing PPP **56**

5.3 ALICE **57**

5.4 AIOTI **58**

5.5 Summary **59**

6 Views of the Expert Groups **60**

6.1 IoT/CPS Expert Group View **60**

6.2 5G Expert Group View **63**

6.3 Big Data Expert Group View **65**

7 Policy Issues **67**

7.1 Privacy and Data Protection Issues **67**

7.1.1 5G 68

7.1.2 Big Data 69

7.1.3 Cyber Physical Systems / Internet of Things 69

7.2 Security issues **69**

7.3 Standards issues 70

7.4 Spectrum issues 70

8 Barriers 71

8.1 Smart Cities 71

8.2 Smart Transportation 72

8.3 Smart Energy and Smart Grid 74

8.4 Barriers for Large and Small Companies 75

9 Concluding Remarks 76

10 References 78

List of Figures

Figure 1. Bringing Together of Views to Identify Potential Opportunities for Collaboration 11
Figure 2. Approach Adopted to Data Gathering 13
Figure 3. Interview Questions 29
Figure 4. Breakdown of Sectors Covered 30
Figure 5. Companies Interviewed 31
Figure 6. Public Private Partnerships 54

List of Tables

Table 1. Smart Cities - Potential Areas for Collaboration 17
Table 2. Smart Energy and Smart Grids - Potential Areas for Collaboration 19
Table 3. Road Transportation – Potential Areas for Collaboration 21
Table 4. Rail Transportation – Potential Areas for Collaboration 21
Table 5. Aerospace Transportation – Potential Areas for Collaboration 22
Table 6. Marine Transportation – Potential Areas for Collaboration 23
Table 7. 5G – Potential Areas for Collaboration 24
Table 8. Big Data – Potential Areas for Collaboration 25
Table 9. CPS/IoT – Potential Areas for Collaboration 27
Table 10. Number of Identified Recommendations for Collaboration per Area 28
Table 11. Summary of Key Messages from Interviews 52
Table 12. Summary of Key Recommendations Identified 53

Acronyms and Definitions

Acronyms	Defined as
ACER	Agency for the Cooperation of Energy Regulators
ADAS	Advanced Driver Assist Systems
AIOTI	Alliance for the Internet of Things
AIS	Automatic Identification System
ALICE	Alliance for Logistics Innovation through Collaboration in Europe
AMP	American Maritime Partnership
ANSI	American National Standards Institute
ARPA-E	Advanced Research Projects Agency–Energy
ARRA	American Recovery and Reinvestment Act
ARTEMIS-IA	Advanced Research and Technology for Embedded Intelligence and Systems Industry Association
ASC	Amsterdam Smart City
CAA	Civil Aviation Authority
CCS	Combined Charging System
CEER	Council of European Energy Regulators
CEN	European Committee for Standardization (Comité Européen de Normalisation)
CENELEC	European Committee for Electrotechnical Standardization
CPS	Cyber-Physical Systems
CPSoS	Cyber-Physical Systems of Systems
CPS PWG	Cyber-Physical Systems Public Working Group
C2C	Car to Car
C2C-CC	CAR 2 CAR Communication Consortium
C2I	Car to Infrastructure
DARPA	Defense Advanced Research Projects Agency
DoD	Department of Defence
DOE	Department of Energy
DOT	Department of Transportation
DSM	Digital Single Market
EASA	European Aviation Safety Agency
EC	European Commission
ECDIS	Electronic Chart Display and Information Systems
ECJ	European Court of Justice
ECSEL-JU	Electronic Components and Systems for European Leadership programme
EEA	European Economic Area
EERA	European Energy Research Alliance
EFTA	European Free Trade Association
EIP	European Innovation Partnership
EIP – SCC	European Innovation Partnership on Smart Cities and Communities
EISA	Energy Independence and Security Act of 2007
EIT	European Institute of Innovation and Technology
eMBB	enhanced Mobile Broadband
EMSA	European Maritime Safety Agency
ENSG	Electricity Networks Strategy Group
ERA	European Railway Agency
ERTMS	European Railway Traffic Management System
ESOs	European Standards Organizations
ETI	Energy Technology Institute
ETNA	European Transport Network Alliance
ETP	European Technology Platforms

ETSI	European Telecommunications Standards Institute
EU	European Union
FAA	Federal Aviation Administration
FCC	Federal Communications Commission
FERC	Federal Energy Regulatory Commission
FP7	7th Framework Programme
FOAs	Funding Opportunity Announcements
FTC	Federal Trade Commission
GSM	Global System for Mobile
GSMR	Global System for Mobile Communications – Railway
HPC	High Performance Computing
HVAC	Heating, ventilation and air conditioning
IBS	Integrated Bridge Systems
ICT	Information and communications technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IERC	IoT European Research Cluster
IIC	Industrial Internet Consortium
IIOT	Industrial Internet of Things
IMO	International Maritime Organization
IOS	Interoperability Specification
IoT	Internet of Things
IoTSF	Internet of Things Security Foundation
ISO	International Organization for Standardization
IT	Information Technology
ITA	International Trade Administration
ITL	NIST Information Technology Laboratory
ITS	Intelligent Transport Systems
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
JPO	Joint Program Office
JTC	Joint Technical Committee
KIC	Knowledge and Innovation Community
LTE	Long Term Evolution
MAF	Maritime Architecture Framework
MIF	Maritime Industries Forum
mMTC	massive Machine Type Communication
MOU	Memorandum of Understanding
MQQT	Modular QPSK to QAM Transcoder
MQTTS	Message Queuing Telemetry Transport for Sensors
M2M	Machine to Machine
NAS	National Airspace System
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NCCOE	National Cyber-security Center of Excellence
NGO	Non-Governmental Organization
NIBIB	National Institute of Biomedical Imaging and Bioengineering
NiCE	Networking Intelligent Cities for Energy Efficiency
NIH	National Institutes of Health
NIST	National Institute of Standards and Technology
NBD-PWG	NIST Big Data Public Working Group
NITRD	Networking and Information Technology Research and Development
NFV	Network functions virtualization
NSF	National Science Foundation

NSTC	National Science and Technology Council
ODI	Open Data Institute
OECD	Organisation for Economic Cooperation and Development
OEM	Original Equipment Manufacturer
OMG	Object Management Group
OPC-UA	Open Platform Communications - Unified Architecture
PPP	Public-Private Partnership
RANaaS	RAN-as-a-Service
RFI	Request for Information
RFID	Radio Frequency Identification
RTOs	Research and Technology Organisations
SAE	Smart Everything Everywhere initiative
SDN	Software-Defined Networking
SESAR	Single European Sky ATM Research programme
SET Plan	European Strategic Energy Technology Plan
SGCC	Smart Grid Cyber-security Committee
SGIP	Smart Grid Interoperability Panel
SMEs	Small and Medium-sized Enterprises
SoS	System of systems
SRA	Strategic Research Agenda
Tbps	Terabit per second
TEN-T	Trans-European transport networks
TERN	Trans European Road Network
TIFIA	Transportation Infrastructure Finance and Innovation Act
TPP	Transatlantic Trade Partnership (Pacific Region)
TRL	Technology Readiness Level
TSIA	Trade Sustainability Impact Assessment
TTIP	Transatlantic Trade and Investment Partnership (Atlantic Nations)
UAS	Unmanned Aircraft Systems
UAV	Unmanned Aerial Vehicle
UL94	Standard for Safety of Flammability of Plastic Materials for Parts in Devices and Appliances testing
URLLC	Ultra Reliable Low Latency Communication
US	United States of America
VPN	Virtual Private Network
VTSS	Vessel Traffic Service Systems
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
WG	Working Groups
3GPP	3rd Generation Partnership Project
4G	Fourth Generation
5G	Fifth Generation

1 Executive Summary

The aim of this report is to bring together opinions, analyse EU-US industrial drivers and encapsulate the societal needs/barriers from a range of sources, and from this put forward initial proposals for collaboration opportunities. These proposals act as input to the Expert Groups and will be considered, refined and prioritised in the next phase of PICASSO as shown in Figure 1.

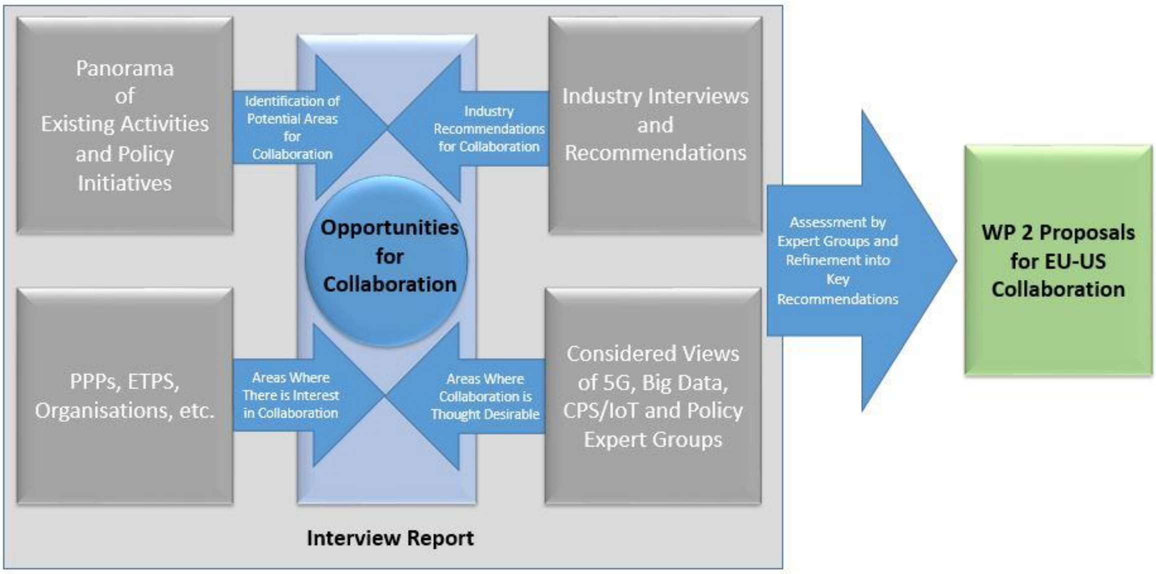

Figure 1. Bringing Together of Views to Identify Potential Opportunities for Collaboration

As a starting point the D1.3 "Panorama of ICT landscape in EU and US: ICT, Policies, regulations, programmes and networks in the EU and US" deliverable was first considered as this gives an overview of key activities in the EU and US and also the relevant programmes in the rest of the world. This was analysed and collaboration opportunities were considered. The analysis highlighted 15 areas where it may be possible to collaborate on research and policy, 16 areas where there is an opportunity to work together on regulations and 9 areas where it would be beneficial to work together on standards.

A major exercise was then undertaken to perform interviews with key industrial actors from large, mid-cap and SME companies from the EU and US in the Smart Cities, Smart Transportation and Smart Energy sectors. In total 150 key actors were approached for the questionnaire and over 70 face-to-face interviews were conducted. The questionnaire was also made available via the PICASSO website. The interviews focused on societal challenges and the PICASSO application domains: Smart Cities, Smart Energy and Smart Transportation, but also included elements related to technological issues, needs, trends and funding needs. Information was also gathered on both industrial drivers and barriers to exploitation, e.g. regulations, lack of standards, lack of business models, etc. The results of the questionnaires were analysed resulting in a total of 61 recommendations being identified. The most fertile areas for collaboration were identified to be in Smart Transportation with a total of 12 areas. Smart Cities was the next most fertile area with 6 areas identified. The area of IoT/CPS is covered by a number of sectors represented notably the Chemical, Automation, Diagnostics, and Information Technology industries plus representation also from other sectors. Considering technologies the area of wireless telecommunications was also a fertile area with 6 areas being identified.

It was notable that industry made very specific recommendations linked with on-going initiatives, e.g. Industrial Internet Consortium, Industrie 4.0 and OPC-UA. However, some common themes were put forward by different industrial sectors in terms of the needs for standards for interoperability of interconnects, wireless communications, protocols and for data exchange. An overriding message was one of the need for data governance, clarity on data ownership and regulation for privacy and the strong need for security. Notably there was good correlation with the collaboration opportunities identified from analysis of the Panorama of existing research activities and those put forward by industry. Additionally, however, industry identified a shortage of skills and a need for agreement on appropriate EU-US skills accreditations.

The opinions from relevant ICT PPPs, ETPs, Clusters and KIC ICT were also sought. The SmartGrids, ETIPWind, ARTEMIS, HPC, KIC-ICT, ENIAC, EPoSS, euRobotics, NEM, NESSI, Networld 2020, Photonics 21, Manufacture, ACARE, ALICE, ERRAC, ERTRAC, Waterborne and IoT Cluster were all contacted. The responses obtained highlighted a range of needs with particular emphasis being placed on the research agendas that have been put forward for the different entities. The questionnaire was also circulated to the Expert Group members and their feedback was collected. Overall there was considerable consensus on what the key issues are.

Considering the sociatal domains there are key opportunities in the areas of Smart Cities and IoT/CPS which are rapidly developing areas and where there are common research, regulatory and standardisation needs. There are also great opportunities in the areas of Smart Energy and Smart Transportation, however, here there is existing regulation and legislation which needs to be harmonised. For the underlying technologies, which are the basic building blocks of future applications: 5G, Big Data and IoT/CPS, there are many opportunities to work together which would allow bilateral access to EU and US markets and would allow technology and products to be sold on the world stage increasing the competitiveness of EU and US companies in existing and developing markets.

2 Introduction

2.1 Objectives, Scope and Data Gathering Approach of the Deliverable

This Public Version of Deliverable, D1.5, provides an analysis of EU-US industrial drivers and societal needs/barriers. The objective of this deliverable is to set the scene for the project execution and provide initial proposals for collaboration opportunities which will be discussed by the Expert Groups. A key aim is to gather as many recommendations as possible and ensure that there is a wide consultation. Of course not all recommendations can be pursued and the Expert Groups will refine and prioritise the proposals into a set of key proposals. Here the analysis has deliberately not looked in-depth at the specific technologies that are being explored by the Expert Groups as these will be analysed at Expert Group level. The Technical and Policy Expert Groups have, however, also provided their views in response to the questions that were put to industry in the questionnaires. The aim of this was to ensure that all views were gathered, those from the technical and policy domains, those from industry and those from analysis of existing research activities, into a single document which can then be used as reference input for future discussions.

Figure 2. Approach Adopted to Data Gathering

The approach to data gathering is shown in Figure 2. The first stage was to perform an analysis of the areas that are already being pursued in the US and EU. This was done via desk work with the collection and analysis of various initiatives, research programmes, policy activities and standardisation efforts that already exist at the EU level, in some EU member states and in the US in the areas of Smart Cities, Smart

Mobility and Smart Grid, etc. A full list is provided in D1.3 “Panorama of ICT landscape in EU and US: ICT, Policies, regulations, programmes and networks in EU and US” [1]. This deliverable considered activities within the EU and US and also at a world-wide level where relevant. This has been used to produce an understanding of key topics, societal needs and policy gaps that need to be considered. This has been analysed and the results are presented in Section 3. The key research, policy and standardization needs are also highlighted.

Interviews were then carried out with industry on both sides of the Atlantic. The aim was to collect opinions on the industrial and societal drivers, the opportunities for collaboration and also where it may or may not be possible to consider collaboration, and at which level. Although the interviews focused on societal challenges and the application domains, elements related to technological issues, needs, trends and funding needs were also solicited. Information was also gathered on both industrial drivers and barriers to exploitation, e.g. regulations, lack of standards, lack of business models. The questionnaire was circulated to key industrial actors and was also made available on the PICASSO website. In total 150 key actors were approached for the questionnaire. By far the most effective way of getting a response was via face-to-face interviews and this also produced some interesting discussions that led to further information being provided. Originally it was planned to perform 20 face-to-face interviews but in practice a total of 70 face-to-face interviews were conducted. This included industrialists from large, mid-cap and SME companies in the EU and US operating in the Smart Cities, Smart Transportation and Smart Grid sectors. Further industry responses (15) were obtained via direct response to the questionnaire. The questionnaires were also circulated to relevant ICT PPPs, ETPs, Clusters and KIC ICT. Responses were obtained from 10 organisations providing additional information particularly in the area of the research priorities. Although the aim of this report is not to go into depth in terms of the PICASSO technical domains the Technical Expert Groups (22 members) were also asked for considered responses to the questionnaire. To cover cross-cutting policy issues the Policy Expert Group (6 members) also considered the questionnaire and identified key policy issues that need addressing. In total the responses from 113 people and 9 organisations are considered.

The deliverable is organised into five main sections. The first section provides the key messages that have been extracted from D1.3 considering the panorama of existing activities being performed in Europe and the US. A table of recommendations and proposals for collaboration is presented. The second section presents the results of the interviews and responses to the questionnaire from key actors in the ICT domain and industrialists from large, mid-cap and SME companies. Again the recommendations identified are summarised in a table at the end of the section. The third section presents the opinions of relevant PPPs that responded to the questionnaire and key collaboration opportunities highlighted are summarised. In the fourth section the considered views of the Expert Groups in each of the technology domains and also with respect to policy are presented along with their recommendations. The final section provides a summary of barriers that were identified for the societal domains: Smart Cities, Smart Energy and Smart Transportation. Additionally, the interviews with industry highlighted some cultural business barriers between the EU and the US. Although it is unlikely that these can be addressed it is useful to understand that these barriers exist when considering the way forward.

3 Analysis and Key Messages from the Panorama Report D1.3

As a starting point the Deliverable D1.3 “Panorama of ICT landscape in EU and US: ICT, Policies, regulations, programmes and networks in the EU and US” [1] was analysed to highlight key areas with respect to policy, research and standards where collaboration may be beneficial. The report provides an overview of industry-driven programs, priorities, networks, and major projects in the EU and US in the areas of 5G Networks, Big Data, Internet of Things and Cyber- Physical Systems. As these areas are also actively being pursued at the world level relevant major programmes around the world are also identified. Key work with respect to regulations and standards is highlighted for each of the domains.

Considering challenges increased urbanisation is seen as a key challenge for the future. It is predicted that by 2050, the world population will reach nine billion with a fundamental shift in demographic towards a more elderly population. The expectation is that 60% of the population will be older than 50 and that 75% of the population will live in cities. This will create great challenges to provide energy supply, logistics, health care, security, food and water. The growing rise in the use of ICT to provide interconnectivity, information and optimisation of services is leading to many “Smart” solutions being proposed. The key areas addressed in the report are:

Smart Cities: The area of Smart Cities includes many potential topics. In this domain ICT supports the efficient use of space, infrastructure and other resources in cities, e.g. integrated smart transportation concepts, lighting, smart garbage collection, optimising use of water and energy, monitoring for safety and the well-being of the inhabitants. It can also include governance, education and the monitoring of citizens health.

Smart Energy: ICT is exploited in many areas within energy supply and is used to provide availability of services, and management to reduce consumption and CO2 emissions. It is used for the stable operation of grids using secure communication systems with automatic load balancing and rejection of attacks, for incorporation of renewables within the main supply and also increasingly for interacting with grids for demand-side management. Smart energy usage is also being enabled within smart factories and smart homes to provide improved energy efficiency in buildings and production.

Smart Transportation: ICT is being used in Smart Transportation to provide an optimised use of infrastructure to increase capacity and also to improve the safety of road transport. This is being achieved through sophisticated traffic management systems that are relying on increased connectivity between cars and between cars and infrastructure. In the longer term the introduction of increased autonomy will lead to fundamental changes to traffic operation.

Considering the technological Expert Groups, the key technologies that are important for the future are:

5G: 5th generation wireless systems will be the next major phase of mobile telecommunications standards going beyond current 4G/IMT-Advanced standards offering data rates of 1 gigabits per second for several hundreds of thousands of simultaneous connections with extremely low latency of less than 1 ms. This coupled with reductions in energy consumption will enable massive sensor deployments in future.

Big Data: Big Data analytics covers the processing, analysis and use of very large data sets to extract value for data to provide trend detection, decision making, greater efficiency, cost reduction, risk reduction, crime and disease prevention, or to provide services to citizens.

IoT/CPS: The Internet of Things (IoT) is used to describe the network of physical objects, e.g. devices, vehicles, buildings, embedded electronics, software and sensors and network connectivity. Here objects can collect and exchange data allowing objects to be sensed and controlled remotely across network infrastructure to improve efficiency, accuracy and provide economic benefit. When feedback is introduced combining sensors with computing and actuators then Cyber-Physical Systems are created allowing control of Smart Cities, Smart Grids, intelligent transportation systems.

In the following sections the areas covered in D1.3 are analysed and suggestions are presented for potential areas for collaboration. This includes opportunities for performing joint research, opportunities for working together at a policy level and for working together on standardisation. For more detailed information on the initiatives and full references readers should refer to D1.3.

3.1 Smart Cities

Within the Smart Cities domain the report highlights the wide range of areas where “smartness” can be exploited including government, economic and financial systems, building management, manufacturing, education, community and social services, healthcare, transportation, utilities and infrastructure, and communications. In Europe a number of initiatives, e.g. The European Initiative on Smart Cities and The European Innovation Partnership for Smart Cities and Communities is investing in sustainable development in as many cities as possible. Key to this is partnership and the aim is to create equal partnerships between cities and companies. The EC is supporting this by creating “Lighthouse Projects” with the intention of these signalling numerous follow-up projects across Europe. Smaller cities are also being aided by the Small Giants Initiative. To support development there is a need for “at scale” experimental research facilities such as SmartSantander and partnerships between companies, governments and knowledge institutions such as Amsterdam Smart City (ASC) (100 partners). Notably there are different levels of “smartness” and there are a large number of cities in Europe (468) which display some attributes of Smart Cities.

In the US the White House Smart Cities Initiative is investing over $160 million in federal research. NITRD has set up a framework to coordinate Federal Smart Cities activities, agency investments and outside collaborations. A number of initiatives are being supported by NIST including the Global City Teams Challenge. Underlying this is foundational research supported by NSF that supports design and management of Smart and Connected Communities. There are a number of notable Smart Cities in the US including Boston, New York, Seattle, San Francisco, Washington, San Jose and Chicago.

The Smart Cities industry is valued at more than $400 billion globally by 2020. Providing technology and services for Smart Cities around the world is thus a major business opportunity and this is a major driver for some national programmes, e.g. in the UK, Japan, South Korea and China. There are many deployments around the rest of the world where best practice could be gleaned.

There are a number of barriers to deployment. There is a critical need for regulation in the area of privacy and in allowing sharing of data to provide services. Smart Cities will constantly register and process private data from individuals leading to questions about gathering data with consent and reconciling the value of services with privacy. Anonymising data, encryption and processing in encrypted domains may all be needed. The very wide scope of Smart Cities, which covers not only interactions with citizens and use of their data, but also control of the energy, waste, transportation systems and social interactions with government, education and e-health, leads to many areas were regulation may be required. Safety is of underlying importance to citizens.

There are several developing standards for Smart Cities (notably in the UK) covering a variety of Smart City topics, ETSI Smart City standards targeted at mobility, transportation, M2M, energy efficiency, security, and ITU-T on Smart Sustainable Cities. China is also very active in standardisation with a number of Chinese bodies.

A growing problem is susceptibility to cyber-attack and here lessons can be learned from countries such as Estonia who have developed world renowned expertise in this domain. In the US NIST is working with the National Cyber-security Center of Excellence (NCCOE) to provide cyber-security solutions based on commercially available technologies for Smart City applications.

3.1.1 Smart Cities - Potential Areas for Collaboration

Research/Policy	Integration of mixed criticality systems – combining the CPS and IoT worlds
Research/Policy	Cyber-Security – bringing together expertise in Europe, e.g. Estonia, The Internet of Things Security Foundation (IoTSF) UK and the National Cyber-security Center of Excellence
Research/Policy	Demonstration at scale and replication of solutions
Research/Policy	Anonymising data, encryption and processing in encrypted domains
Regulation	Regulation in the area of privacy and in allowing sharing of data to provide services
Regulation	Changes to allow new methods of certifying systems for safety
Standards	Development of Smart City Standards and providing guidance and best practice on implementation of smart functionalities
Standards	Interoperability, e.g. Smart City standards targeted at mobility, transportation, M2M, energy efficiency, security and ITU-T on Smart Sustainable Cities.

Table 1. Smart Cities - Potential Areas for Collaboration

3.2 Smart Energy and Smart Grid

Energy and Smart Grids are key topics in both Europe and the US driven by national and European green initiatives, e.g. in Europe to reduce greenhouse gas emissions by 40%. Urban areas consume 70% of energy, and account for 75% of the EU's greenhouse gas emissions. Thus buildings, transportation systems, water supply and treatment, and sewage management are an area where most energy savings could be made. Notably nearly 50% of European Smart City initiatives address environmental problems. The European Strategic Energy Technology Plan (SET Plan) has identified the need for development of energy technologies to combat climate change and the need for securing energy supply at the European and global level. To support this the European Energy Research Alliance (EERA) has been set up by leading European research institutes and the SETIS Initiative has been created to support cities and regions in sustainable use and production of energy. An ICT Roadmap for Energy Efficient Neighbourhoods has been created and KIC InnoEnergy has been set up as a commercial company dedicated to promoting innovation, entrepreneurship and education in the sustainable energy field.

At a national level policies are also driving change, e.g. in Germany to phase out nuclear power and in the UK cutting greenhouse gas emissions by 80% by 2050. The low carbon economy strategy in the UK is driving the setup of public private research partnerships and a range of initiatives for electivity and heating. Every home will be supplied with a smart meter helping consumers to understand their energy consumption and make savings.

In the US as part of the Reinvestment and Recovery Act there are a number of government initiatives and policies including $3.4 billion of investment grants for Smart Grid projects. This includes funding to promote energy-saving choices for consumers, increasing efficiency, and fostering the growth of renewable energy sources such as wind and solar. The Energy Independence and Security Act of 2007 (EISA) also made it policy to modernise the nation's electricity transmission and distribution system to create a smart electric grid. This is supported by the Administration's commitment in the "Blueprint for a Secure Energy Future" and "A Policy Framework for the 21st Century Grid: Enabling Our Secure Energy Future."

Around the world different approaches are being adopted and a wide variety of technologies and services are being demonstrated driven by national and regional business drivers. In the US peak load reduction technology and dynamic pricing tariffs are being pursued. In Europe emphasis is on improving energy efficiency and reducing emissions through the decentralised production. In the Asia-Pacific region China is modernising and improving grid reliability and Australia and New Zealand are exploring new techniques for load management. There are major investments in China ($128 billion) to reduce carbon intensity by investment in renewable power and to create grid interconnectivity with neighbouring countries such as Russia, Mongolia, Kazakhstan, Pakistan, Myanmar, Laos, Nepal and Thailand. Since 1992 China has relied heavily on electricity it purchases from Russia. Other countries also actively pursuing Smart Grids are Brazil, Mexico, South Korea and Japan.

The Smart Grid market is led by regulation and reductions in emissions, consumer choice and energy security are driving adoption of Smart Grid technologies. Regulation across Europe is introducing smart metering and tariffs. A number of pricing structures are being explored: tiered pricing rates that reflect system capacity and time-of-use pricing (off-peak/on-peak) schemes. Introducing "Critical Peak" prices has been found in a US pilot to be the most effective technique to trigger load reduction.

Across Europe grid regulation varies considerably making Smart Grid investments difficult. In Europe the Electricity Directive and the Energy Services Directive provide a mix of obligations and incentives to Member States to establish a common regulatory framework. Other bodies also need to be involved such as the Agency for the Cooperation of Energy Regulators (ACER) that fosters cooperation among European energy regulators to ensure market integration and the harmonisation of regulatory frameworks within the framework of the EU's energy policy objectives and the Council of European Energy Regulators (CEER) that represents national regulators.

In the Smart Grid area there is a need for standards for interoperability and safety. Standards are voluntary in Europe and are developed by industry and market actors. The European Commission and EFTA have issued the Smart Grid Mandate M/490 which was accepted by CEN, CENELEC and ETSI. In the US EISA asked NIST and FERC to facilitate the development and adoption of interoperability standards. NIST is leading this coordinating the development of a framework that includes protocols and model standards for information management to achieve interoperability of Smart Grid devices and systems.

Security is another key concern and smarter grids lead to increased vulnerabilities from intrusions, error-caused disruptions, malicious attacks, destruction, and other threats. As the electric grid network is key to the operation of a country, cyber-security is a key topic on both sides of the Atlantic. The European Commission has put together a multi-stakeholder and multidisciplinary group of experts to discuss and work on relevant matters regarding the security and resilience of communication networks and information systems for Smart Grids across Europe. Although standards for Smart Grid cyber-security are already available these need to be maintained and enhanced as technology evolves. In Europe Alstom Grid, Intel, and McAfee produced a white paper on Smart Grid cyber-security. In the US the Administration has proposed specific cyber-security legislation to ensure that grid operators and all stakeholders have access to actionable threat information and provide support for research, development, and demonstration of cyber-security systems. The aim is to identify and prioritise relevant cyber risks - including malware, compromised devices, insider threats, and hijacked systems - and develop standards and guidelines that enable the design of effective plans for mitigating those risks. A number of threat warning bodies have been set up in the US, Electricity Sector – the Information Sharing and Analysis Center, the United States Computer Emergency Readiness Team, and the National Electric Sector Cyber-security Organization. The NIST Information Technology Laboratory (ITL), Computer Security Division leads the Smart Grid Interoperability Panel (SGIP) Cyber-security Committee (SGCC) which has produced the NISTIR 7628 Guidelines for Cyber-Security (Volumes 1, 2, and 3) that are widely used by utilities, vendors, and regulators in the US.

3.2.1 Smart Energy and Smart Grids - Potential Areas for Collaboration

Research/Policy	There are many synergies in research and policy in the areas of smart metering, energy efficient neighbour hoods, Smart City energy management, low carbon economy and renewable energy. There may well be opportunities for joint research.
Research/Policy	In the area of cyber-security closer ties should be encouraged between the European Commission multi-stakeholder expert group and the NIST Smart Grid Interoperability Panel (SGIP) Cyber-security Committee (SGCC). Here there are critical lessons to be learned from expertise in Estonia and from the US guidelines, e.g. NISTIR 7628.
Regulation	Sharing of best practice regulation for smart metering and tariffs to manage system load capacity (off-peak/on-peak schemes).
Regulation	Introduction of harmonised regulation to allow stakeholders to make grid investments in EU and US.
Standards	Currently standards for interoperability are being driven by the European Commission and EFTA, e.g. the Smart Grid Mandate M/490 which was accepted by CEN, CENELEC and ETSI. EISA in the US has asked NIST and FERC to facilitate the development and adoption of interoperability standards. Here there may be opportunities to harmonise standards development.

Table 2. Smart Energy and Smart Grids - Potential Areas for Collaboration

3.3 Smart Transportation

North America and Europe are expected to be the largest markets for Intelligent Traffic Systems. Within Europe sustainability is a key issue with a dramatic increase in both freight and passenger transport and associated emissions. There is also an aim to halve casualties with respect to 2001 levels in road transport. The European Commission supports a number of transport Technology Platforms that includes ERRAC (Rail), ERTRAC (Road), ACARE (Aerospace) and WATERBORNE (Marine) that sets the research agenda for each domain. At a national level there are several programmes implementing Intelligent Transport Systems for road users. To coordinate the planning of infrastructure projects across Europe the Trans-European transport networks (TEN-T) policy has an investment programme of EUR 400 billion. The European Commission’s aim is to accelerate and coordinate the deployment of ITS applications on the Trans European Road Network (TERN) across Member States in a consistent and harmonised way.

The drivers in the US for intelligent transportation are similar to those in Europe, however, another key driver is homeland security. There is a desire to provide surveillance of roadways and also a means for mass evacuation of people in urban areas as a result of natural disaster or threat. In the US the ITS Joint Program Office (ITS JPO), coordinates across the Federal Highway Administration, Federal Motor Carrier Safety Administration, Federal Railroad Administration, Federal Transit Administration, Maritime Administration, and the National Highway Traffic Safety Administration to plan, programme, and execute the ITS Research Program. This is being supported by a guidance handbook from the SSTI and Smart Growth America and stimulation challenges, e.g. the Smart City Challenge. Looking longer term Beyond Traffic is looking at trends and needs over the next three decades.

3.3.1 Road

The ERTRAC Strategic Research Agenda covers mobility, transport and infrastructure, safety and security, environment, energy and resources, design and production. It highlights a number of key research topics including traffic management, integration of vehicle and infrastructure systems, traffic management using ITS, data collection and processing, business models, optimisation of road space to ensure that vehicles (particularly HGVs) adopt routing systems that minimise adverse impacts, systems for segregating traffic with dedicated infrastructure and prioritised traffic management and methods to assist the booking of optimised slots for freight vehicles. Multi-modal door-to-door mobility is also being considered in the New Mobility Services project. Autonomous driving features to improve safety are being pursued in both Europe and the US with projects like HAVEit, the Swedish Drive Me project and the Google car in the US.

The adoption of electric vehicles and the decarbonisation of transport is a priority in both Europe and the US. In Europe there are a number of “green initiatives” to promote the take up the use of electric vehicles and to reduce pollution across a range of transport modes such as the European Green Cars Initiative and the Smart, Green and Integrated Transport programme and EV4SCC with €6339m funding. In the US the Recovery Act is providing large investments in advanced vehicle and fuel technologies, public transit, and high speed rail. Tax credits are being used to encourage uptake of electric cars. Urbanisation is a key challenge and air quality directives such as Euro 6 are driving new truck and powerplant design in Europe. Likewise stricter standards are being introduced in the USA to raise average fuel economy to 35.5 miles per gallon for cars and trucks by 2016. Within trucking there are particular problems for Europe such as a myriad of automatic tolling systems which would benefit from harmonisation. On both sides of the Atlantic telematics is being exploited to reduce carbon footprint and optimise deliveries by major logistics companies such as DHL and UPS.

Increased connections to cars is being driven by regulation in the EU for the introduction of car emergency vehicle notification systems (eCall). Standards for car-to-car and car-to-infrastructure communication need to be global to allow automotive companies to sell their products around the world. The ITS market is global and there are many opportunities in the Asia Pacific region and India. In the EU the CAR 2 CAR Communication Consortium has been developing and testing standards driven by the EC M/453 mandate for European standardisation organisations ETSI, TC, ITS, and CEN to produce a minimum set of standards that ensure interoperability. Likewise in the US there is a focus on vehicle-to-vehicle and vehicle-to-infrastructure connectivity through the application of advanced wireless technologies. The ITS Research Program is developing and testing the underlying technology and applications. The ISO/TC 204 standard particularly addresses intelligent transport systems, with a focus on standardization of information, communication and control systems for urban and rural surface transportation.

3.3.1.1 Road Transportation – Potential Areas for Collaboration

Research/Policy	There are many similarities in policy in the EU and US driven by climate change and increased urbanisation. There are opportunities to collaborate on Intelligent Transport Systems, autonomous cars, electric cars and alternative fuels.
Regulations	As the automotive market is global there are opportunities to harmonise regulations that promote adoption of green technologies, e.g. electric cars and reductions in fuel consumption and emissions.
Regulations	There is a need to address barriers to the adoption of autonomous cars at a global level. This requires regulation on safety, liability and also privacy.
Standardisation	Wireless standards are needed for ITS, for car-to-car and car-to-infrastructure communication. These need to be world-wide as the marketplace for automotive manufacturers on both sides of the Atlantic is global.

Table 3. Road Transportation – Potential Areas for Collaboration

3.3.2 Rail

The interoperability regulations and the 2011 Transport White Paper require that the European railway system behaves as a single network. The commercial drivers in the industry are for 24/7 operation, high availability, low cost, safety, increased capacity, recovery from disturbance, low carbon emissions and customer satisfaction. In Europe the Strategy for European Rail Research – Vision 2020, the Strategic Rail Research Agenda, and "Railroute 2050" vision, highlights the need for the European Railway Traffic Management System (ERTMS) to replace the existing 20 train control systems utilised across the European Union. Key initiatives are the H2020 supported FOSTER-RAIL and SHIFT^{2}RAIL joint technology initiatives to focus research and innovation (R&I). In the US there is a major need to modernise the rail system and although there has been investment of $11 billion on High Speed Rail initiatives this has been largely spent on upgrading the existing Amtrak service which is limited to 110 miles per hour. Although a further $10 billion has been requested by Congress to support high-speed initiatives there is considerable opposition from republican governors and community opposition for projects that are seen as too expensive and unnecessary. Some high speed rail projects are going ahead, e.g. the controversial Los Angeles - San Francisco route, and privately funded initiatives from All Aboard Florida with a $1.5 billion loan from the Federal Railroad Administration and the Texas Central Railway company. This plans to introduce Japanese bullet trains between Houston and Dallas.

3.3.2.1 Rail Transportation – Potential Areas for Collaboration

Research/Policy	There are opportunities for joint research on providing high availability in rail networks, maintenance approaches, emissions reductions and approaches to increasing capacity.
Regulation	Automatic train control systems are already a reality in Europe and will be in place across Europe by 2023. Opportunities within the US may also be considered but regulation is required to support this.

Table 4. Rail Transportation – Potential Areas for Collaboration

3.3.3 Air Transportation

Air passenger volume is predicted to double air traffic density over the next two decades in an already congested airspace. The Single European Sky ATM research programme SESAR is reforming the architecture of European Air Traffic Control to meet future capacity and safety needs. SESAR aims at developing the new generation air traffic management system capable of ensuring the safety and fluidity of air transport worldwide over the next 30 years. The equivalent of SESAR in the US is NEXTGEN. A concern here from a global perspective is that both systems adopt fundamentally different approaches to air traffic management. Autonomous Unmanned Vehicles are very active area on both sides of the Atlantic with many military programmes. Considering civilian programmes there is only one major national programme in the UK, ASTRAEA. In the US there is some activity from Amazon on developing drones for delivering parcels which raises some certification issues with the FAA. These are being trialled in the UK.

3.3.3.1 Aerospace Transportation – Potential Areas for Collaboration

Policy and Research	There are many research projects both industrial and academic exploring the use of autonomous aircraft. Here there may be opportunities for joint work.
Standardisation	In the area of Air Traffic Management there are two different systems being developed in the EU and US respectively. It is important that these are interoperable.
Regulation	There is a need for regulation that allows autonomous aircraft to operate safety in civil airspace – here it would be beneficial for the CAA, EASA and FAA to work together.

Table 5. Aerospace Transportation – Potential Areas for Collaboration

3.3.4 Marine

A key driver in the maritime industry is improving safety of waterborne operations as accidents come with high costs in terms of loss of life, environmental damage and high economic impact. Traffic management is key for safer and more secure operations. The technology can also be used for optimised shipping operations and voyage optimisation, condition based maintenance, reducing costs and reducing emissions which is driven by strict legislation in Europe at a national level and also at the local level in ports. In Europe the WATERBORNE European Technology Platform has defined the Marine Vision 2020 and Strategic Research Agenda which drives funding for projects. There is a major e-Maritime initiative to exploit advanced information technologies within the maritime sector. Unmanned navigation and autonomous ships are also being researched but there are considerable hurdles to adoption coming from regulators concerned about safety and unions who are concerned about job losses. Current regulations dictate minimum crew levels by international conventions.

In the US the Maritime Administration of the US Department of Transportation has highlighted that policy reforms are needed to address international shipping trade. Offices have been created at major US gateway ports to interact with key stakeholders to identify Federal and state funding and cooperate on projects. Public private partnerships are being used to identify bottlenecks and ways of improving freight movement, and to fund redevelopment of port infrastructure, e.g. berths, piers, container cranes, on-site rail and railroad trailers. This is being strongly supported by the Transportation Infrastructure Finance and Innovation Act (TIFIA) programme that provides direct loans, loan guarantees and credit with $1.435 billion in capital over five years.

A strong domestic maritime industry is seen as being critical for America's economic, national, and homeland security. The maritime industry is strongly represented by the American Maritime Partnership (AMP) with 450 members and the Jones Act requires that any vessel transporting goods or passengers between two points in the United States or engaging in activities in US waters must be US owned, US built, and US crewed.

3.3.4.1 Marine Transportation – Potential Areas for Collaboration

Research/Policy	Research on navigation for ships, increased autonomy and emissions reductions.
Regulation	Harmonisation of regulations on emissions, e.g. IMO.
Regulation	Safety regulations are needed to further reduce crew levels and move towards autonomous ships, e.g. minimum crew levels may need to be removed.
Standardisation	EU activities on E-Maritime and MAF need to be harmonised with US activities to allow interoperability.

Table 6. Marine Transportation – Potential Areas for Collaboration

3.4 5G

5G extends the cellular network from content delivery to a 'Control Network' that allows new control applications. The EC has committed €50 million for research to deliver 5G mobile technology by 2020. This includes initiatives like the 5G Infrastructure Public Private Partnership to bring together several telecommunications companies. In the first call for phase 1 a total of 19 5G PP projects were launched and currently Phase 2 proposals are being prepared for 2017. In the US President Obama announced a $400 million Advanced Wireless Research Initiative in July 2016 to boost research for next-generation mobile networks. This will establish four city-sized testing grounds for 5G wireless services from October 2017 with close engagement with industry. Supporting this the Federal Communications Commission voted to make a large block of spectrum available for permission-less 5G development and use.

There is a key need for spectrum harmonisation for 5G so that the same frequencies are used worldwide and companies who operate on a world-wide basis can produce appropriate equipment. Lessons have been learned from 4G LTE where harmonisation was not possible. The US has a dominant lead in 4G LTE but it is not widely deployed in Europe and the rest of the world where the concentration is very much on 5G.

The uptake of 5G depends upon standardisation to be in place, however, the roll out of 5G is expected to be gradual allowing equipment upgrades to occur before some of the key 5G standards are formalised in 2018 and 2019. There are many pre-standards activities going on around the world in 5G with demonstrators from T-Mobile US, Ericsson, Verizon, and large investment from South Korean companies and China with pilots in European countries. Docomo is publicly committed to having a 5G service up and running for the Tokyo Olympics in 2020. To get joint agreement on technical fundamentals and 5G spectrum bands globally by 2018 NTT Docomo (Japan), KT and SK Telecom (South Korea), and Verizon(US) are forming the 5G Open Trial Specification Alliance to drive technology and standards forward. Pre-standard "5G-ready" equipment using software defined network (SDN) technology will allow network operators and enterprise customers to move to upgrade to full 5G once standardisation is in place for spectrum allocation and licences are issued. Other bodies that are likely to influence 5G standards are the Next Generation Mobile Networks NGMN 5G roadmap targeting 2020 for 5G launch, the GSMA to bring together operators, and the ITU for harmonisation.

3.4.1 5G – Potential Areas for Collaboration

Research/Policy	Currently work on 5G in the US and EU is disconnected and fragmented. Efforts to establish collaboration between the 5G PPP in Europe and the Advanced Wireless Research Initiative in the US should be made.
Regulation	Spectrum harmonisation is required at a global level so that the same frequencies are used worldwide (to avoid what happened with 4G LTE)
Standardisation	There are many initiatives driven by large companies such as NTT Docomo, Samsung, Ericsson, T-Mobile and Verizon. There is a need for all companies to work together and this is already happening in initiatives such as NGMN 5G. There is a need for a strong EU-US voice in these initiatives.

Table 7. 5G – Potential Areas for Collaboration

3.5 Big Data

In Europe the Digital Single Market (DSM) and data driven economy is driving many activities on data. The European Big Data strategy has funded over 150 research and innovation projects and the Big Data Public Private Partnership has been set up with many key players. Similarly the NSF Big Data Research Initiative is driving activities in the US with the Cyberinfrastructure Framework for 21st Century Science and Engineering (CIF21) fostering development and implementation of a national cyberinfrastructure for researchers in science and engineering by making data available within different research communities. Several agencies such as NSF, NIH, DARPA and the Department of Defence (DoD) have their own Big Data Initiatives. Policy in the US focuses more on the actual uses of Big Data and less on its collection and analysis. The US wants to lead both in the international arena and at home. The BD2K Centres of Excellence programme has established 11 Centres of Excellence for Big Data Computing. DARPA and the DoD are also actively engaged. DARPA is creating and providing open source the XDATA software toolkits for applied mathematics, data visualization and computer science. The DoD is increasing Big Data-related research and development with all military services funding R&D in the area. The Big Data Technology roadmap is being led by NIST and this is defining requirements for interoperability, portability, reusability, and extensibility for Big Data analytic techniques, and also the technology infrastructure in order to support secure and effective adoption of Big Data.

Critical to maximising the benefits from Big Data is the ability to access and share data. In Europe the Open Cities project and Commons for Europe Project are demonstrating the power of open data as well as the Citadel on the Move project that makes it easier for citizens and application developers from across Europe to use Open Data. At a national level a number of projects such as Open Data Helsinki are showing the promise of open data usage. A key barrier is the ability to share information effectively. There is a need to rationalise Information Governance regimes across public services and to address the semantics of information to allow sharing. There is also a general lack of openness with respect to data around the world as indicated by the Open Data Barometer published by the Open Data Institute (ODI) which covers 88 countries.

The area of privacy is a key topic on both sides of the Atlantic. In the US there is also an accent on policies to strengthen and stimulate US research in practical privacy-related technologies. This is covered by the 14th Amendment of the US Constitution which gives a person the right to determine what sort of information about them is collected and also how that information is to be used. In the marketplace this is enforced by laws intended to prevent deceptive practices and unfair competition. The Privacy Act of 1974 prevents unauthorised disclosure of personal information held by the federal government. In Europe there are different attitudes and regulation with respect to privacy in different member states. In Germany, for instance, privacy is a key concern and is strictly controlled. To try and harmonise the area of privacy the European Data Protection Directive (Directive 95/46/EC) was introduced to protect an individual with respect to processing of personal data and on the free movement of such data. At an international level the "Safe Harbour Privacy Principles" were introduced so that US companies can comply with privacy laws that protect European Union and Swiss citizens. US companies who store European customer data may self-certify that they adhere to 7 key principles. This was challenged and ruled inadequate so a Privacy Shield agreement has been put forward. This is still the subject of intense discussion. In particular, even if US companies have European data centres, cloud services may still require transfers of EU data to the US (or other countries) to provide some features or provide technical support. Encryption is thought to be a way forward. For instance, ID data can be encrypted before it enters the cloud with the data owner keeping the encryption keys. This gets around Safe Harbour and Privacy Shield laws, however, it is expensive and only 1% of cloud companies offer encryption.

Standardisation is a key enabler in the field of Big Data. There are already a number of standardisation initiatives at a world-wide level such as the ISO/IEC Joint Technical Committee (JTC) 1 Working Group (WG) on Big Data, the IEEE Standards Association standards related to Big-Data applications and specifically IEEE P2413, and the ITU "Recommendation ITU-T Y.3600" for Big Data services.

3.5.1 Big Data – Potential Areas for Collaboration

Research/Policy	Big Data and Open Data are both viewed as being essential for the development of many areas. There are very strong policy initiatives on Big Data on both sides of the Atlantic and there are many opportunities for synergies working together at the foundational level and also in terms of engaging with activities such as those at NIST. The area of open data is less clear with many local initiatives at national levels. The lack of open data is currently a barrier to many applications. The power of open data is becoming more apparent from pilot initiatives around the world and this may lead to replication in other cities and countries. The uptake of this is, however, fragmented and initiatives that would allow replication would be beneficial.
Regulation	Regulation is a key enabler in the field for global adoption of services and this is already well recognised with activities such as Safe Harbour and Privacy Shield.
Standardisation	Standardisation activities are already being addressed at an international level and this should be further promoted.

Table 8. Big Data – Potential Areas for Collaboration

3.6 CPS/IoT

The Digital Single Market Strategy and the Digitising European Industry initiative are key drivers in Europe for IoT and CPS with the concept of "Smart Everything Everywhere". There are major initiatives to cluster activities together and support development of platforms. The IERC (IoT European Research Cluster) brings together 40 EU-funded projects with the aim of defining a common vision, identifying common research challenges and coordinating and encouraging the convergence of ongoing work. Likewise the Alliance for the Internet of Things (AIOTI) has the aim of creating a European IoT ecosystem with further IoT Large Scale Pilots being funded to promote IoT take up. There are also major initiatives such as FIWARE which are providing open, public and royalty-free architectures and specifications to allow developers, service providers, enterprises and other organizations to develop products. This is cross sectoral with 16 Future Internet Accelerators addressing Smart Cities, E-Health, Transport, Energy and Environment, Agrifood, Media and Content, Manufacturing and Logistics, Social and Learning.

In the US Developments in IoT are largely being driven by companies with major players Google, Cisco, etc. dominating the marketplace. The Department of Commerce is promoting growth of the digital economy and as part of the Digital Economy Agenda, the National Telecommunications and Information Administration is initiating an inquiry to review the current technological and policy landscape for IoT and issue a “green paper”. This will highlight potential benefits and challenges, and possible roles for the federal government in fostering the advancement of IoT technologies in partnership with the private sector. Various consortia and alliances have been formed to promote the uptake of IoT. These include the US Industrial Internet Consortium (IIC), the Allseen Alliance (dedicated to providing and open environment for the Internet of Things) and the Open Interconnect Foundation founded by major companies (Intel, Microsoft, Samsung, Qualcomm, GE Digital and Cisco Systems) working on IoT chips, software, platforms and products with the aim of working together towards a single standard for IoT.

The importance of IoT is recognised world-wide and large investments are being made in a number of countries, e.g. the Korean Government is investing $350 million in 300 companies it thinks can compete globally in the next four years, to develop an IoT ecosystem.

Within Europe there are many projects on CPS and the EC strategy has been to cluster these with clusters being formed on CPS and Systems of Systems. To bring industry together in the areas of micro-/nano-electronics, embedded and Cyber-Physical Systems and smart systems the ECSEL-JU has been set up. Supporting this the ARTEMIS Industry Association (170 members) is also funding large projects such as CRYSTAL on interoperability and EMC on mixed-criticality systems. Competence centres have also been set up to engage with SMEs. At a national level the Industrie 4.0 programme is driving work on CPS in manufacturing.

In the US work on CPS is being driven by the NSF Cyber-Physical Systems programme which has funded over 300 projects. Here basic CPS research is being addressed that can be used across multiple application domains and NSF is working closely with multiple federal government agencies. The NITRD CPS SSG is responsible for coordinating programmes, budgets, and policy recommendations for Cyber-Physical Systems (CPS) research and development (R&D). Although a number of federal agencies have independent research efforts it has been identified that there are still many gaps in the federal R&D portfolio. The NIST Cyber-Physical Systems and Smart Grid Program Office is leading NISTs activities on Cyber-Physical Systems. A Public Working Group (CPS PWG) has been formed and a CPS Framework has been developed in partnership with industry, academic and government experts. This provides a methodology for understanding, designing and building CPS. NIST also lead the Global City Teams Challenge to help communities around the world work together to address issues including air quality, traffic management and emergency services coordination.

Key challenges are interoperability of systems to allow easier integration of highly complex systems. There is a need to provide standards and regulations that support the creation of an ecosystem of developers and users of CPS and IoT systems. Here a harmonisation between the US and Europe is not only advantageous but strongly needed. Regulation also has a crucial role in the development of CPS and IoT. IoT deployments at scale have many implications including implications for privacy (applications rely on collecting and utilising data from a myriad of sensors) and security where the increasing interconnectedness of systems leads to vulnerabilities to unintentional errors and cyber-attacks. There is also a need for business models and regulation to support market access.

3.6.1 CPS/IoT – Potential Areas for Collaboration

Research/Policy	Engineering trustable, reliable, evolvable and affordable cyber-physical systems connected by the Internet of Things is a scientific and technological challenge that requires huge efforts and where joining forces will help to advance more quickly and thus meet societal challenges. At the same time it would enable US and European companies to compete in world markets.
Research/Policy	Integration of mixed-criticality systems – combining the CPS and IoT worlds.
Research/Policy	Provide guidance and best practice on implementation of smart functionalities.
Regulation	Regulation (changes) will be needed to allow new methods of certifying systems for safety.
Regulation	CPS/IoT deployments at scale have many implications, including implications for privacy (applications rely on collecting and utilising data from a myraid of sensors). Regulation on privacy and the sharing of data regulation has a crucial role in the development of CPS and IoT.
Regulation	The interconnectedness of systems leads to vulnerabilities to unintentional errors and cyber-attacks. Regulation is needed with respect to security.
Regulation	There is a need for business models and regulation to support market access.
Standards	There is a need to provide standards for interoperability that support the creation of an ecosystem of developers and users of CPS and IoT systems. Here a harmonisation between the US and Europe is not only advantageous but strongly needed.

Table 9. CPS/IoT – Potential Areas for Collaboration

3.7 Conclusions from Analysis of Panorama Report

There are many similarities in programmes being pursued in Europe and the US and many commonalities in the drivers behind these which in many cases are global. It is also clear that there are a number of opportunities where joint collaboration between the EU and US would be beneficial. In total the preceding analysis identifies 15 areas where it may be possible to collaborate on research and policy, 16 areas where there is an opportunity to work together on regulations and 9 areas where it would be beneficial to work together on standards.

Area of Collaboration	N. of Identified Recommendations
Smart Cities	8
Smart Energy	5
Smart Transportation	13
▪ Automotive	4
▪ Rail	2
▪ Aerospace	3
▪ Marine	4
5G	3
Big Data	3
CPS/IoT	8

Table 10. Number of Identified Recommendations for Collaboration per Area

Considering the collaboration opportunities by area (See Table 10) the most fertile domain for collaboration is Smart Transportation with a total of 13 identified areas across the automotive, rail, aerospace and marine sectors. Notably, however, there is less scope for collaboration with respect to the rail sector. The area of Smart Cities is also a very fruitful domain for collaboration with 8 areas identified. This corresponds to major initiatives in both the EU and US. The area of Smart Energy is highly regulated and there are key differences in infrastructure and standards within the EU and US which makes collaboration less easy. Considering the technological areas, CPS/IoT is the most fertile area for collaboration with 8 areas identified which reflects the wide coverage of the CPS and IoT domain in terms of applications.

In the next section the responses from industry to the PICASSO questionnaire are considered. Here of interest is whether these match the current priority topics being addressed by the programmes being performed on both sides of the Atlantic. Also of interest is whether there are other topics raised by industry that are not currently being addressed.

4 Industry Interviews

Interviews were performed in order to get the views from industry leaders and key actors operating in the fields of interest to PICASSO. The original intention was to perform face-to-face interviews with industrialists from around 20 large, mid-cap and SME companies in the EU and US operating in the Smart Cities, Smart Transportation and Smart Grid sectors to gather opinions with wider coverage being obtained through circulation of the questionnaire to a larger number of key actors. In practice face-to-face interviews proved very fruitful for data gathering and so 70 face-to-face interviews were performed. The questionnaire was also additionally sent to 80 key industrialists. In total around 150 people were contacted and there were 85 responses from a wide range of industry sectors.

PICASSO
EU-US ICT collaboration

- What is/are the application domains that you are interested in, e.g. Smart Cities, Smart Grid, Smart Transport, etc.?
- What do you see as the societal trends that are driving this area?
- What are the industrial drivers for this domain?
- Are there any policy drivers for this domain?
- Are there any current barriers to exploitation, e.g. regulations, lack of standards, lack of business models?
- What are the technologies that you are particularly interested in, e.g. 5G, Big Data, IoT/CPS?
- In your opinion what are the key technological issues/barriers that need addressing?
- What in your opinion are the funding priorities for this area?
- Where do you believe it is possible for the EU and US to collaborate?
- Where do you think it is not possible for the EU and US to collaborate?

Figure 3. Interview Questions

The questionnaire is shown in Figure 3. The questions were targeted at identifying the areas of interest for industry, societal trends driving the area, the industrial drivers for the area and also any policy drivers that exist. The questionnaire also asked about perceived barriers to exploitation in terms of regulations, standards, or from a business perspective. These are areas where PICASSO may be able to make recommendations to circumvent key barriers. The interests of industrialists in particular technologies were also canvassed as well as the technological issues that needed addressing. Looking forward, interviewees were also asked about the perceived funding priorities in the areas and where they believed it would be possible and necessary for the EU and US to collaborate. A final question was added to also identify any areas where interviewees felt it would not be possible to collaborate. The last question, in particular, highlighted a number of issues and problems from previous attempts at collaboration.

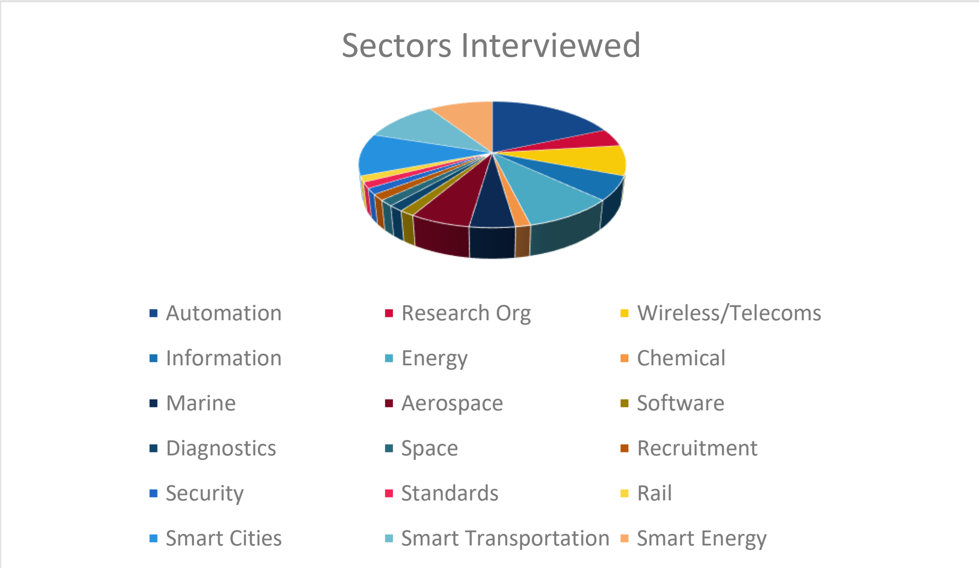

Figure 4. Breakdown of Sectors Covered

The industry sector coverage is shown in Figure 4. Care was taken to ensure that there was input from as many relevant sectors as possible. Here it can be seen that there was considerable interest in the areas of Smart Cities, Smart Transportation and Smart Energy from a number of companies (particularly the larger companies). There was a very good response from the automotive, aerospace, automation and energy sectors in general. The views of the recruitment sector were also obtained as it was noted by a number of companies that skills and education are key requirements for the future digital workforce.

4.1 Overview of Companies Interviewed

Figure 5. Companies Interviewed

Examples of the companies that were interviewed are shown in Figure 5. A mix of companies was selected from large well known internationals to smaller SME's to provide balance. Smaller SMEs are likely to be much more innovative in providing new solutions, whilst larger companies have capacity and presence to roll out technologies on a large scale. It was notable that many companies, both large and small, had an interest in Smart Cities, Smart Transportation and Smart Energy. The actual comments from companies or organisations are anonymised in the report and are not attributed unless permission was specifically granted. It should be noted that the face-to-face interviews also provided considerably more material than presented here. Very specific information that would compromise anonymity has been omitted. In the following sections the responses have been gathered together and combined into the sectorial domains identified in Figure 4.

4.2 Smart Cities

As noted in the Panorama report the area of Smart Cities covers a diverse range of topics and it is sometimes difficult to separate out sub topics such as Smart Grid and Smart Transportation due to the strong symbiosis between domains. It was notable that several large companies, e.g. Honeywell, GE, Thales, IBM, CISCO, etc. expressed an interest in several topics including Smart Cities, Smart Grid, Smart Buildings, Smart Transportation and Critical Infrastructure in general. The societal trends identified by companies driving this area are reductions in greenhouse gas emissions, the needs for clean air and water, and the need for increased security and safety. There are also societal benefits from e-Health and also from commerce driven by the ability to use connectivity for collaboration. Policy drivers in this area are tax breaks for companies to support city connectivity and the increasing move towards collectives and hubs for city connectivity. From an industrial perspective, considering topics such as clean air and water or security and safety, there is demand from both consumers and governments. Here companies see an opportunity and are seeking to satisfy needs with both products and services. In particular, there is increasing demand from customers for green-house gas mitigation driven by policy. In the US legislation and executive orders have been implemented, and in Europe there are a number of directives and targets that have been set. A current barrier to exploitation is the fact that the CO_2 footprint of conventional systems is not factored into prices. This is seen as a major barrier to developing cost-effective and clean alternatives which complicates the challenge of devising effective business models. Regulations and standards already exist in a number of areas, but they are not globally harmonised which limits exploitation. A key requirement for the future is interoperability of different products and systems to enable wider implementation. It was noted that often nominally following the same standard does not result in interoperability. At a technological level the area is currently being driven by networking technologies and this is seen as the “glue” for success. 5G, IoT, Big data, Software Defined Networking (SDN) and Interdomain SDN are all seen as key technologies that are needed. The main barriers are spectrum allocation, privacy and security. Provision of privacy and cybersecurity were seen, in particular, as key to exploitation.

It was noted that Big Data is of interest across a number of sectors, e.g. Smart Cities, Smart Grid and Smart Transport, driven by societal trends in mobility, portable sensors, energy awareness and mobile applications. Here there is a trend towards information availability for faster and better decision making. The industrial drivers for this domain are coming from efficiency for large corporations who provide services such as electricity and water. There are needs for interoperability and this is linked to supply chain management. There are also opportunities for small business but here there is a need to identify suitable business models based on exploitation of data. To support this at policy level there is a need for open government policy on data. The key technological issues/barriers that need addressing are to provide a data interoperability infrastructure (similar to network communication protocols) that enables data mashup. Here there is currently a lack of initiatives to allow/encourage/enable city network hubs.

The policy drivers for the domain are very dependent on national considerations (politics). Here funding to address enabling technologies and applications development as well as tax breaks for connectivity were advocated. The current barriers to exploitation include regulations, lack of standards and lack of business models. There are also ethical issues, in particular privacy of data, and this is driving the domain at policy level. Already there are major funding schemes in place, e.g. in the US, the National Science Foundation has a major initiative in CPS. For collaboration it was suggested that areas where competitive conflicts are less likely such as in the areas of energy, air, and water are pursued. Areas where there are large business opportunities in the near term would also be more difficult to collaborate on. There are, however, opportunities for the EU and US to collaborate in a number of areas such as a common/standard data interoperable infrastructure (e.g. Named Data Networking for the Future Internet), Big Data analytics as a service, joint applications development, data sharing, data movement, network protocols, spectrum allocation, research on inter-domain SDN, identity management, cloud computing interoperability, privacy and security. An area where it is thought difficult to collaborate is in the area of privacy as the approach is different on both sides. Here there is a need for “balanced” cooperation. A noted concern from European actors was that in the US the law is that all software developed in the US shall be given to the NSA for “US add-ons”.

4.3 Automotive Sector

In the automotive sector the areas of electromobility, autonomous vehicles and intelligent traffic management were all highlighted by companies and research organisations as being important. In addition to the development of more efficient electric vehicles and battery technologies there is a key need to develop the infrastructure to support charging as this is seen as the current barrier. There is already considerable joint work going on between the EU and US (e.g. JRC with the Argonne National Laboratory and United States Department of Energy) developing interoperability of charging stations. Working jointly in this area is a key requirement and a Letter of Intent was signed in 2011 between Argonne and JRC to create a common work programme. Electric vehicle charging needs to be able to work seamlessly across the world and in a variety of different conditions, e.g. at different extreme temperatures experienced. Already 70 different types of charging station have been tested. The aim is to come up with a specification for testing of charging stations so that people can travel across Europe. There is also a need for new billing approaches and this area is already advanced in Europe driven by funding from DG Move.

Considering the technologies being addressed in PICASSO it was noted that Big Data methods are important for identifying the locations of potential charging stations and also for advising drivers of their current energy status and how to get to the most appropriate charging stations. Already work has been done using terabytes of insurance company data collected from existing diesel/petrol cars to analyse how many people could live with an electric car in the future. Based on typical travel habits of drivers it is also possible to work out the best places to locate charging stations.

A current funding priority in the area of electric car testing is for instrumentation for cars to monitor efficiency of driving style and the demands on energy for HVAC, etc. in different regions, so that reliable range data can be provided. Already the automotive industry has been tarnished by the “diesel scandal” and so a lot of work needs to be put into providing appropriate and trustable legislation and regulation based on precise numbers for efficiency and range. There is also a need to develop approaches for fast charging (ABB for instance are looking at fast charging for buses where the bus is recharged in 1 minute) and a Combined Charging System (CCS) standard for connectors for interoperability. Looking further to the future there is a need to address wireless charging where there are currently a lot of quasi standards. There may also be opportunities for new services such as bidding schemes to provide charging to customers. It was notable that large companies are also very interested in coordinated car charging and here large companies such as IBM are promoting software solutions already.

Another key interest from automotive manufacturers to reduce accidents in the future is the move towards autonomous road vehicles. Notably this is being driven by the desire to make cars safer and reduce accidents rather than societal pull for the technology. It was highlighted that customers are suspicious of the technology so there is a need to build trust. The traditional industry players are keen to show that they have the latest technology, however, as yet the business case for full autonomy is not clear. There could be fundamental changes within the sector and in the future people my want to avoid the hassle and responsibility of owning a vehicle altogether and rather order personal transport as and when required by phone. At a policy level governments believe that autonomy makes for safer roads and greater transport efficiency with the assumption that the technology challenges will be solved. The traditional OEMs are pursuing an incremental approach to autonomy which will increasingly make the role of the driver one of supervision with periodic interventions to cope when the system limits are reached. A challenge is that the human factors experts have highlighted that people are really bad at intervening successfully in an emergency so there is the possibility that there will be an increase in accidents as the technology is deployed more widely.

The current barriers to exploitation include regulation. The law (Vienna Convention of 1968) currently requires the driver to be in control. Testing of autonomous vehicles is being allowed by exception in particular jurisdictions. The question of insurance and legal liability in the case of accidents has yet to be resolved. Practically the adoption of full autonomy will require lots of real world data, e.g. map data to high levels of resolution and data collected in real time by all the vehicles on the road to cope with hourly\daily changes in road conditions. The key technological issues and barriers that need addressing are in environment sensing that copes with all environmental conditions, e.g. changes in lighting and atmospheric conditions.

Other large companies engaged in smart infrastructure development highlighted the needs for systems engineering and interoperable interfaces for roadside infrastructure. It was noted that the introduction of autonomy and intelligent traffic management also requires changes in engineering practices between OEMS and suppliers. Integration work is required going down through the supply networks. Key technologies required to support this are sensor technologies, approaches to mixed criticality, interoperability of tools, integration of engineering domains and integration of different disciplines across the supply chain. The policy driver in the domain is legislation to reduce deaths, however, the introduction of autonomous driving will require new regulations and currently the issues of product liability and lack of standards are problems. Fundamentally the business models of OEMS will need to change. The priority areas are seen as Big Data, IoT/CPS, sensor technology testing and validation (V&V). In the first instance a European Automotive standard is needed. It is expected that this would influence the rest of the world and would eventually lead to a global standard. The areas of systems analysis and V&V were highlighted as being particularly important and this is reflected in the ARTEMIS-IA Strategic Research Agenda. An example here is the need for testing of Downloaded Apps for driving in the future.

4.4 Aerospace Sector

The area of autonomous systems in the aerospace sector is not a new concept and it was noticeable that this area is already very active with work in both the military and civil sectors in the EU and US. At the small drone level it was not clear where there was a need for cooperation, however, there is a need for certification approaches for larger UAVs. This is currently being addressed at national levels and there could be benefits from international approaches. Notably a major breakthrough would be reduction in certification cost as current requirements for certification and the need for a pilot in command make larger aircraft expensive to produce and operate. The adoption of larger aircraft would open up new applications.

It was noted by the larger industrials that there are other areas where it would be possible to collaborate. Large companies rely on global supply chains and an area where there is an opportunity for collaboration was in the area of Smart Factories / Factory of the Future which is being driven by CPS/IoT. The societal trend driving this is a need for skills and competence in the sector and also the need to look after the well-being of workers inside factories. The areas of energy and sustainability were also cited as being of interest. The industrial drivers in the sector are performance, flexibility and quality. The policy drivers include legal aspects like privacy of individuals and social relationship in the enterprise.

It was noted by industry that currently there is a shortage of skills and here there is a need for the appropriate skills and competences to be developed within universities to supply the future work force. A number of barriers to exploitation of new technologies were highlighted including regulations, lack of standards and lack of business models. Within the sector there is interest in the PICASSO key technological areas: 5G, Big Data, IoT/CPS, and also model based system engineering. Here the ability to produce a 3D “digital twin” of a product was highlighted as well as the need for IT security to protect against cyber-attack and industrial spying.

Many companies, e.g. engine manufacturers, already provide product services and have implemented sophisticated aftermarket support services based on collection of terabytes of data daily. Here there are opportunities to provide some of the data that is being collected to create new services which can be offered to operators. Already Google, for instance, provide information from private pilots in the US on wind speeds and direction which is collected from existing aircraft. The key technological issues/barriers that need addressing are security and the ability to provide large scale deployment of data driven services at low or acceptable cost. It was noted that it would be possible for the EU and US to collaborate on autonomous systems, model based systems engineering, IT security, and aerospace oriented solutions for the factory of the future. All of these are considered to be funding priorities.

4.5 Maritime Sector

It was noted that connectivity and new ICT technologies are currently revolutionizing the maritime industry. Significant new business opportunities arise from using information technology in the domain as there are numerous complex economic and social-technical systems with many different actors and stakeholders. The increase in maritime traffic from international transportation of goods is also driving the growth in IT-Systems to enable safer shipping. The maritime domain historically utilises paper charts. The advent of the Automatic Identification System (AIS) and Electronic Chart Display and Information Systems (ECDIS) have led to enhanced maritime safety. Currently, however, there are different systems in place at the regional, national and global levels leading to a large number of fragmented, heterogeneous maritime IT-systems. There is a need for a common approach across the maritime domain to support the development of interoperable, dependable and secure maritime cyber physical systems. This requires harmonised, standardised system architectures, based on commonly agreed concepts, methods, tools and technology.

At the policy level the IMO and its e-Navigation Strategy is creating a harmonised information exchange between several maritime stakeholders to make maritime transportation safer and more efficient. A number of new systems are being introduced for e-Navigation such as Integrated Bridge Systems (IBS) and networked Vessel Traffic Service Systems (VTSS). These Cyber-Physical Systems are transforming the way humans and ships interact with the physical world. In Europe work is focussed on the Maritime Architecture Framework (MAF) which provides conventions, methods, languages and tools to document, align, design and handle existing and future system architectures and architectural reference models within the maritime domain.

There is also considerable interest in increased ship automation. This is being driven by the Cruise Vessel market which is rapidly growing, particularly in China. The levels of automation are increasing and there is some discussion at present on remote autonomous operation and the application of mobile robots. To support this there is a need to have regulations to allow autonomous operations of marine vessels. There is also a need for future automation system architectures to be more open. For this standardisation will be key and this is seen as the key barrier that needs addressing.

Another clear trend is towards electrical propulsion for ships, including having a DC grid (Low Voltage or Medium Voltage) on board the ship which potentially saves substantial amounts of fuel. The policy drivers for this are the International regulations on energy efficiency and emissions control.

As these technologies are currently being introduced the areas where there are needs for research and development are in development, testing, validation and verification of new e-Navigation solutions. Additionally, there is a need for testing infrastructure to prove new technologies and a need to deploy test systems and perform sea trials. Standardisation is a common problem for both automation systems and also for autonomous operations and here there is an opportunity for collaboration.

4.6 Rail Sector

In the rail industry there are few opportunities to harmonise systems in terms of rolling stock as this is dictated by large companies that manufacture the trains. The area of infrastructure is also highly regulated. Already there are key players in this area and standards exist. There has been considerable effort across Europe to harmonise the rail network and the most advanced area, ERTMS for automatic train operation, is already well developed. This is being rolled out across Europe with significant infrastructure investment committed. This standard is also being used in other countries. Looking to the future the opportunities for joint collaboration exist in areas where there is currently a research interest. One area cited was the area of the Smart Grid for railways. Here there is an opportunity for joint work on harmonisation between Europe and America in the area of renewables and energy storage. A challenge at present is that it is necessary to get insurance for liability and in the US there is a need for special contracts which makes doing business difficult. Although the CE trademark is universally accepted across Europe it is not accepted in the US. Thus there is a need to produce customised products for the US market which is a barrier to trade.

Another area where there are opportunities, particularly highlighted by SMEs, is in the area of monitoring. There is an opportunity to sell both hardware and software solutions and services. It was noted by some companies that sell worldwide that a particular challenge is the need to comply with UL safety standards in the US. Additionally, although European companies have very competent people with good qualifications they need to give further specific training in order to meet US health and safety requirements. Harmonised safety standards at a world-wide level were thus seen as advantageous. It was noted that security as yet has not been a key issue but will be in the future.

4.7 Space Sector

The space sector is keen to deploy satellite technology to support developments in Smart Cities and Smart Transport. Here there is an opportunity to use remote monitoring and communications to reduce congestion in urban areas and provide information services. In addition to increased urbanization other changes in the world will also impact congestion such as the on-going fourth industrial revolution. The increasing use of digital technologies and 3D printing will make the decentralised production of goods possible. This will result in a global change in transport needs. This trend will affect goods manufacturing and maintenance, energy production and distribution, as well as communication networks.

The societal drivers for adoption of new technologies will be demands for reduction in energy wastage and emissions from being stuck in traffic jams, demands for reductions in the delays that people suffer and demand for customized products. At a societal level evidence of global warming, an increased interest in the ecology and a desire for improved balance between personal and professional life is driving this. The future is seen as an increase in self-employment, better work life balance and more autonomy. The benefits will be reductions in pollution and stress, increased choice and also economic gains. All of these changes will have to be properly accompanied with strong policies.

The main industrial drivers are the need for efficient communication networks with high data rate and accessibility from various locations, the need of new tools to better understand the overall situation in terms of business opportunities (e.g. demands for a specific product), transport needs and traffic situation, and the need for sharing of goods and services more easily.

4.8 Energy Sector

The area of energy is seen as a fertile area for new technologies driven by a number of initiatives in Europe and the US. Companies were interviewed across the sector with both major players and smaller equipment providers being canvassed. Overall there was a lot of pessimism in the sector with respect to opportunities for collaboration. Considering the very large companies, e.g. GE, there is interest in all aspects of Smart Cities, Smart Transportation and Smart Grids. Sub-tier companies highlighted the needs of switchgear, charger monitoring systems and peak power transformers. There was also interest in integrating renewables within the grid such as wind power chargers for electric cars to create smart greener cars. Other companies had more specific offerings for asset management, protection settings management, asset diagnostics, energy monitoring for efficiency using software and Apps for existing products such as air conditioning, heating buildings, controlling electric motors, compressors and drives. Underlying this some companies were concentrating on providing telecoms for the electricity industry. It was highlighted that the interest in telecoms and Smart Grid was world-wide with customers in South East Asia, the Middle East, Mexico and Brazil.

A challenge with developing systems for the US is that the topology of the network in the US makes it very difficult to implement a Smart Grid. In the US some parts of network are 100 years old. In Europe the oldest parts date from the 1950s (as a consequence of reconstruction after WWII). The problems of trying to meet different certification standards were highlighted by many companies. Although the functionality being provided for systems is virtually the same the differences between the EU and US mean that variants of technologies have to be produced. European companies particularly highlighted the barrier of US certification standards, e.g. UL certification. The IEC standard is not compatible with UL94**.** Some companies use UL standards for low voltage products, e.g. protection systems and measuring gear, and use IEC standards for high voltage products. A fundamental problem is that **i**n the US is that there are bigger differences between potentials. As a consequence EU manufacturers need to develop totally new products for the US market. This places European companies at a disadvantage compared to US suppliers. In order to get UL certification it is necessary to pay US inspectors. An example was given of one device that cost 40K Euros to certify and then subsequently the factory needs to be re-certified every year at a cost of 1500 Euros. The need for this annual recertification of European manufacturers per product was not clear. It was noted that the US was a huge potential market, however, in addition to the IEC and UL standards differences, a further barrier are the regulations for fire protection which are different in the US. This means that the materials used to make products have to be non-flammable in the US which is different to Europe. Here again it is necessary to pay for a certificate for products.

As a consequence smaller companies highlighted that it was easier to operate in European markets so they did not have plans to sell to the US. To get around the existing barriers some large companies such as GE have set up production facilities in Europe to manufacture to European standards. For the European market GE manufactures its lower voltage and medium voltage hardware in Poland. Any displays, however, required are supplied from the US. An unusual approach adopted by GE in order to meet the differing requirements of Europe and the US is that they have projects in Germany which utilise German project management, however, the manufacturing is performed in the US. By using this approach they can sell products in both markets.

Looking to the future it was highlighted that the requirements for Smart Grids in the US are so different to those of Europe that it is unlikely that it will be possible to synchronise requirements between the two continents. Here it was felt that the standards were unlikely to come together as there are significant differences in the distribution networks deployed. An example is that in the US overhead lines are used whereas in Europe the electricity lines tend to be underground. Also it was noted that the demands in the US for Smart Grid are very difficult to meet. Although Funding Opportunity Announcements (FOAs) for Smart Grid had been issued by the DOE nothing was continued as companies struggled to deliver what was requested. Work in the US is now mainly continuing via local initiatives, e.g. with Montgomery council. The most pressing need is to rebuild the electrical network in the US which is not a need in Europe.

Companies that sell world-wide highlighted that the world is divided into standards. In addition to the EU-US standards issues it was noted that the Asian market was also a significant challenge as the requirements vary dependent on client. Thus global harmonization of standards would be a significant benefit to companies. However, this is complicated by the fact that standards are set by a variety of different bodies. In Europe for instance standards are defined by CEN-Cenelec and by national efforts. This makes collaboration and agreement of standards at a global level difficult.

There is also a move towards renewables in the energy generation sector targeted at Smart Transportation, Smart Buildings and Smart Homes. The sector is being driven by the decarbonisation of transport, environmental and noise pollution and also the subsidised uptake of Photo Voltaics. Here there are needs for wind turbines, solar protection and Smart Grid products with opportunities in both the electrification and automation of Smart Grids. The challenges in the sector are the high demands for quality, repeatability and performance. For this, the key interest is in using real-time data for optimal energy management to control devices such as smart blinds, etc. At present the different standards for electrical products in the EU and US are proving to be a barrier to adoption. In the area of integration of renewables Big Data and IoT are considered to be very important with a need for intelligent connectivity and the ability to deal with huge amounts of data to manage energy. It was noted by industry that although there is a lot of discussion there is a need for action. The renewables sector is a very competitive area and a challenge for companies is to achieve a suitable ROI considering very strong competition from China. It was noted that the competition from China was very well organised and directed so there is a need for the EU and US to work together to compete.

Looking to the future companies are investigating superconducting connections for engines, cables, current limiters and motors generators. It was highlighted that the energy sector is a highly regulated market which makes innovation very difficult. There are two key challenges when trying to introduce new technologies. The first is that there is resistance to innovative ideas and the second is that the industry wants technology that has been proven (in some cases proven for 50 years). Although new superconducting technologies can offer much higher efficiencies, particularly for public grids, it is very difficult to convince regulators that the technology is proven. Here there is a fundamental “chicken and egg” problem in that how can the reliability of the new technology in a grid be proved when regulators will not allow it to be installed so that it can be proved? It was noted that the electricity supply sector is highly standardized and it would be good to have a world-wide standard. In some cases the existing standards are a barrier. For instance, the standards for safety levels for current and voltage preclude the use of ceramics in new products. If the standards were more flexible then there could be more innovation. Here it was felt that the utilities companies need to look at the risk involved in changing the existing standards. If this was done then it would also be good to develop a global standard at the same time.

In the industry major initiatives such as Industrial Internet Consortium and OSP Consortium Cloud platforms are seen as the future. Already GE is promoting the concept of CurrentbyGE which is a platform for Smart Cities. In the area of communication for future Smart Grids the IIoT (Industrial Internet of Things) consortium is trying to develop global standards. The big issues for the future were highlighted to be security and data management. In particular, there is interest in data for industrial use cases. It is thought that the machine data privacy issues here are less sensitive than those of consumers although encryption is still very important. To provide this the larger companies are buying in security technology for their platforms. It is also important to have only one owner of data.

4.9 Automation Sector

The area of automation is very active with great interest in the Internet of Things and key initiatives such as Industrie 4.0 in Germany. There is a major opportunity for automation of field assets. Here there is a need for the supporting network and control infrastructure. Many companies interviewed, both large and small, highlighted that the IIoT will be a key technology for the future. Large companies also highlighted that they have internal initiatives to support this. In addition to the automation of things, monitoring was also seen as key driver for the industry. There are many new ideas being promoted such as the “augmented operator” where information is provided to smart devices/mobile phones. This is being used to provide information for optimisation, asset management and predictive maintenance to operators as they walk around the factory. At a policy level drivers in the industry are local legislation and emissions rules. In general, a lot of data is generated during manufacturing leading to an interest in Big Data. Companies that concentrate on manufacturing components that are safety-critical, e.g. for the automotive and aerospace industries, generate large amounts of data that needs to be collected and stored.

Within the industry there is a need for interoperability and standardisation. As there are so many different equipment manufacturers and the need to interconnect with existing legacy systems there is a need for integration interoperability particularly in the area of fieldbuses. A number of companies (particularly SMEs) highlighted the need for companies to move away from proprietary solutions that are designed to lock out competition. The production of Industrie 4.0 compatible automation products is seen as an opportunity for harmonization within the industry. In the future the expectation is that the cloud will be used to connect smart components.

The increased use of decentralised control is foreseen with the move to Industrie 4.0. In Europe although Industrie 4.0 is very high profile and is mobilising the industry it is felt that the value has not yet been demonstrated. For communications the IIoT is seen as the way forward by larger companies. It was noted that being part of the Industrial Internet Consortium is seen as being a PR boost for a company which explains why so many companies are signing up to this. It was also highlighted that OPC-UA is a major new standard in the automation industry that is gaining popularity. At a practical level the area of wireless communications is problematic with the need to support many different wireless standards and work with hybrid wireless networks.

To avoid problems of privacy and data security a number of approaches are currently used. This includes storing all data on site at customers and providing local data centres in both the US and Europe to avoid problems of data transfer. To avoid data privacy issues all European data is kept in European data centres and all technical support is provided in Europe. It was also noted that in production systems for applications such as aircraft or pills there is a need for long term data storage **(**30 years).

When exploiting telecommunications and real time data there is a need for cyber security and this needs to be at all levels. Industrial cyber security is seen as a key issue. The need for security needs to be traded off against “Openness” which is seen as being quite risky. There is a need to provide tamperproof access on the web for products and more and more companies are providing encrypted data for customers.

It was highlighted that experience is that in the US the customers have a clear idea of what they want when it comes to automation. In Europe quite often this is not the case which means that customers are more often led by solutions providers.

Considering opportunities for collaboration it is thought that it is potentially possible for the EU and US to work together in all areas, however, the reality is that there strategic interests that may prevent this. A challenge is to find partners who are willing to collaborate. There is a need for regulation, and to provide guarantees of QoS and reliability. Research in the area of IoT is a key requirement and there is a need to collaborate and develop joint standards. Here large companies are performing work either in Europe or the US. An interesting problem highlighted was the difficulty in selling secondhand equipment to the US. In the industry it is quite common to resell old robotic and manufacturing equipment to other factories as an existing factory is updated which makes for a more sustainable business model. Importing of “used materials” to the US is a real problem made difficult by US transparency and security requirements which effectively creates a barrier to this sustainable business model.

A significant subdomain of the automation sector is the chemical process control sector. Companies working in the chemical sector highlighted a trend towards smart flow measurement and control solutions. Here a fundamental problem is in meeting different regulations in Europe and the US. Even harmonisation of regulations across Europe would be beneficial. Several companies commented on the difficulty of selling equipment to plants around the world where different standards are in place.

It was highlighted that chemical plants are never turned off so there is a need for high availability and monitoring to support this. Increased automation is seen as a way of reducing operators and allowing 24/7 operation without the need for night shift operators. A key problem in the near term is that half of existing refinery workers will retire in the next few years. These workers have years of experience of optimising the existing assets. New engineers do not have this experience. There is thus an opportunity for automation systems and optimisation of processes based on much greater collection of data. A challenge is to decide where to add sensing technology to get the best payback. An example here was it would be possible to monitor flicker on light bulbs so an alert could be made to indicate that a bulb would fail about 100 hours later so that maintenance could be scheduled, however, the cost and energy used to achieve this would not make it economic. It was noted that for every KW used in a factory it is actually necessary to generate 3KW so there are big savings to be made particularly in the area of energy.

4.10 Diagnostics and Plant Monitoring

The area of diagnostics is an actively growing area with a number of very large companies developing capabilities to support their existing products. Also notably there are many SMEs engaged in this market providing data gathering/analysis systems and services. Some SMEs provided data solutions across a number of different sectors providing predictive and prescriptive analysis in the banking and insurance, telecoms, manufacturing, energy, transport and retail sectors. Here there was great interest in the use of embedded IoT for predictive maintenance. In some cases larger companies had gone into partnership with smaller companies to provide monitoring services for their products, e.g. smart vibration alarms with self-learning capability for condition based monitoring. For looking at plant efficiency there is increased interest in exploiting cloud and fog technologies. There are a number of opportunities for providing sensors, SDKs and platforms that provide a device cloud. Building upon this it is possible to perform large-scale data ingestion and aggregation utilizing Big Data technologies on time series data. Scalability is an issue and it is necessary to handle a billion events a day from a million devices so the scale of the problem is a challenge. The key requirement for the future is seen to be platform standardization. It was noted that for the smaller companies, in particular, it is a challenge to make money out of data. In terms of technology a number of approaches are being used to gather data. Some companies provide their own hardware but it is more common to just provide software. Some larger companies highlighted that they had engineers and developers in both Europe and the US but tended to produce hardware only on one continent. For transferring data a number of approaches are used and currently a lot is being done using 2G to transfer data for on-condition based maintenance. New technologies with more capability and bandwidth open up new opportunities.

Key areas for the future were highlighted as being energy management, process control and predictive monitoring. Several companies had produced tools that collect data which is then put in the cloud. Another area which is becoming important is in the use of smart tags for tracing components through a factory. A key requirement for this is encryption. The Smart Factories Consortium also highlighted the need for predictive maintenance. In this sector companies highlighted the difficulty of trying to support many different proprietary protocols. A number of standards are coming to prominence such as OPC-UA for interfacing and also IBM as a standard for cloud systems. Interoperability is seen as a key requirement for the future and it is thought that there will be a merging of standards within Industrie 4.0. It was noted that big companies set standards and many of these are proprietary. There is a need for Open Source and for rapid development with a need for industry to push technologies much like Android has done for phones. Critically there is a need to be quick. For the future the IIC is seen as very important for diagnostics.

In the safety monitoring area there is a need for protective monitoring and knowledge-based condition and performance monitoring solutions for rotating machinery in the hydro, oil, gas and wind sectors. Online condition monitoring is increasingly being used for monitoring safety and performance. In this sector security is now the key issue and this is becoming more important than the data. The area of security is being considered under IT Industrie 4.0. The current approach to using the cloud is for companies to deal with data security and privacy issues locally in each country. Harmonisation in this area would make it easier to develop products that can be sold easily across borders. It was noted that Industrie 4.0 is developing sensors that talk directly to the cloud. This will be a major step change for the industry which will need appropriate security mechanisms in place.

4.11 Information Technology Sector

The area of information technology is dominated by companies such as SAP, ATOS and IBM. These companies highlighted interests in Smart Cities, Smart Energy, Smart Transportation and Smart Manufacturing. However, they also indicated much wider interests in healthcare, retail, banking, mining, oil and gas. The societal trends driving the Smart City area are a change of world demographics with a migration to cities and influx of a young population with typically a high usage of social media. The industrial drivers for this domain are the advent of smart devices, mobile technology and networks. The area is being driven by Public Private Partnerships but the main barrier to exploitation across multiple European states are different national priorities. The technologies of particular interest are Big Data, mobile communications and IoT. The key technological issues/barriers that need addressing are data privacy and confidentiality. The funding priorities for this area are Big Data Analytics and the sharing of data with privacy provisions. Areas where it was believed that the EU and US could collaborate are in applications of Big Data in Health Records and Homeland Security. However, it was not thought that collaboration in terms of joint funding is possible in the sector.

Interoperability is seen to be key and as a consequence companies such as ATOS are strongly supporting the Industrial Internet Consortium. Companies also see Industrie 4.0 being very important for the future and highlighted the gathering momentum for OPC OA. For the future there is a need to consider privacy and security and already projects such as the Industrial Data Space (which involves 12 Fraunhofer Institutes) is addressing this area. The need for Governance of data as a product was advocated. In the future there will be a need for data brokerage between providers and users. The brokers will need to be certified in some way. Another key issue is data ownership. This needs to be supported with data stewardship and also controls on the purchasing of data need to put into place.

4.12 Wireless/Telecoms Sector

The wireless/telecoms sector was characterized by a mixture of large companies, e.g. Ericsson, Huawei, AT&T and Cisco addressing mass market applications and SMEs targeting niche applications. A very large number of potential applications were highlighted which included GSMR for the rail sector, general video surveillance in many domains, infotainment and condition monitoring for the maintenance of cars, and secure communications for autonomous driving with connectivity for ADAS. 5G was seen as important for Smart City applications: including home automation, communications for white goods, smart parking, outdoor lighting, waste management (whether a bin is empty or full to avoid unnecessary collections); energy supply (the Smart Grid domain for substation automation and smart meters); and industrial and process automation for manufacturing.

In terms of technology the large American companies highlighted interests in 3G and 4G applications. AT&T have significant activities going on in Europe and have their own interface to Brussels. The company is particularly promoting Smart Cities, the Internet of Things and cyber security. The approach they are adopting is called Prevent Detect and Respond. It was noted by networking providers that providing the interconnectivity for specific devices also opens up the ability to provide WiFi coverage to other users/potential customers. For the future there is a need for global standards. Here there is interest in Profinet and Ethernet IP and already switches have been developed with multiple interfaces to allow interoperability.

European and Chinese companies highlighted their interests in 5G. Already 25Gbits/s data transmissions rates have been demonstrated and it is expected that standards will be in place for 5G by 2019. In the area of Smart Traffic Management it was highlighted by Ericsson that the company has developed a “Connection Traffic Cloud” which is used by 16 traffic management centres in Germany and they are also working on a connected vehicle cloud for Volvo. A key technology highlighted that was necessary for the future was network slicing for virtualization. This makes it possible to provide different settings on the same hardware so that different slices can be assigned different bandwidths dependent on the needs of applications.

Considering the future there is strong competition from Chinese companies. Huawei for instance highlighted that the company is working on narrowband IoT. A sensor with interfaces has been produced based on 5G technologies with a target to provide a battery life of 10 years for applications such as water meters. Notably they have developed an approach where they can monitor the battery power left in devices as this is seen as crucial for remote sensors. The need for standard data was highlighted so that it is possible to easily interface different sensors as in future applications. There will be millions of devices connected at the same time so a scalable approach is needed. Here Huawei’s is promoting a publish-subscribe mechanism.

SME companies from both the EU and US were interviewed that were interested in machine to machine, low-power, wide-area network technologies for the Internet of Things (IoT) and IoT platforms for communications for white goods, building automation and also for machine to machine communications in manufacturing. Here the aim is to use platforms to connect products together and use the data for predictive maintenance. There are many opportunities for SMEs and this includes hardware and software for various end modules, gateways, and network infrastructure for many diverse applications such as HVAC equipment, water heaters, pool equipment, municipal pump down gears, water meters, parking applications, and private and public networks.

US SMEs highlighted that the introduction of 4G LTE has been run by US companies and this has been successful. A challenge for companies is that it is difficult to differentiate products in the home market and it is difficult to sell to Europe as there is a significant difference with respect to hardware and there is a need for quite a lot of effort to tailor to the European market. There is also a need for CE certification to sell in Europe. Harmonisation of technology and standards would be a significant help for small companies. With respect to data storage there are significant issues with respect to Safe Harbour and Privacy shield. This raises questions of where should the data centre be located and having people on site to provide technical support. It was noted that privacy was a key issue in Germany.

SMEs in Europe also highlighted issues of privacy. To avoid issues some companies use the Microsoft cloud in Germany with German Telecom being the data trustee. Others used a data centre in Dublin with IBM software for the cloud. By using European data servers SMEs could concentrate on the key problem which is one of connecting machines together. With respect to data the general approach was to store data wherever and however the customer wanted it. At the machine level the issues of data privacy are not such a concern, however, for personal data there is a need for “Privacy Shield”. It was highlighted that the European data protection initiative is useful in that it provides a level playing field across Europe.

European SME’s tended to sell within Europe and had found difficulties selling in the US even with an American representative. The high costs of UL certification were also cited as an issue. There was a lot of interest in exploiting cloud technologies but there is a lack of standards to support this at present. For example there are no standards for white goods interoperability and this would be beneficial. In general the industry in the automation sector is using OPC–UA but this does not scale well in the cloud. Security was also highlighted as a key barrier for exploiting the cloud. Currently companies tend to employ MQTT and VPN connections.

4.13 Software Development and Tools Sector

In the software domain the primary interest is in IoT related applications. The proliferation of standards and platforms is making life very complex for providers and customers. Key needs are for IoT Infrastructure for Smart Transportation and Industrial applications. The societal trend that is driving this area is the rapid growth in the transportation sector (with a growth rate 2X faster that international trade) and the growth in manufacturing using rare materials and energy. Both sectors produce greenhouse gases. The industrial drivers for this domain are systems intelligence and optimization, energy footprint reduction, preventive maintenance and the opportunity to provide additional services. Policy drivers in the transportation sector regulate safety, security and environmental impact. The main current barrier to exploitation is that there is no IoT standard but rather a proliferation of initiatives (IIT, S3P, Predix, Thingworks, AWS, Azure, M2M, etc.). With respect to software tools the technological areas of primary interest are IoT/CPS. The key technological issues/barriers that need addressing are IoT platform interface standardisation, Embedded Operating Systems standardisation and development of cybersecurity certification standards. It was noted that funding for IoT and CPS should be directed at use case building and platform convergence. The sector highlighted that there was a clear need for the EU and US to collaborate on IoT/CPS. However, an area where it was thought that it is not possible for the EU and US to collaborate is cybersecurity. Already there are a number of issues in the privacy domain with respect to Safe Harbour and technical standards that are being promoted.

4.14 Research Organisations and Networks

Research organisations highlighted a general interest in all the PICASSO domains: Smart Cities, Smart Grid, Smart Transport, but in particular the areas of increased connectivity and increased autonomy which cuts across all domains. The need for research on assurance and cybersecurity was highlighted as being needed for all domains. The societal trends that are driving this area are mobility, connectivity, globalisation and also personalisation of products and services. The industrial drivers for this domain include globalisation, increases in autonomous functionality and advances in Artificial Intelligence. IoT/CPS systems were noted as sometimes being highly regulated which prevents adoption of technologies. A number of areas were highlighted as barriers to exploitation. These include differences in EU and US rules on privacy and use of personal information. It was highlighted that it may be premature to introduce regulations and standards in this area as these might stifle innovation. It was noted that trust will be crucial to exploitation and this is the key current barrier. The key technologies of interest are autonomy at rest, autonomy in motion, persistent connectivity and cybersecurity for IoT/CPS. To address the existing barriers the funding priorities are seen as trust and cyber security. From an academic viewpoint no areas were identified where it would not be possible to collaborate. At a higher level it was thought that it would also be possible to collaborate on research and policy discussions.

4.15 Security and Data Protection

Cybersecurity companies highlighted that there is a need for industrial cyber security as evidenced by the increasing number of cyber-attacks. Large companies highlighted the need for security with the increasing connectivity of systems and many had deals in place with leading cyber security companies such as the Kaspersky Laboratory. Companies working on providing software for data intensive solutions e.g. HMI, web applications, etc., for factory and process automation, maritime technology, mechanical engineering, building automation and the energy sector, all highlighted the need for data protection. Smaller companies were reliant on using products from larger companies, e.g. Microsoft products, and via security services provided by communications companies, e.g. T-mobile. To avoid data protection issues local data centres were being employed, e.g. German data centres for German businesses.

4.16 Standardisation

The need for standards in a number of areas was highlighted by both large and small companies. The IIoT concept which was developed by GE with the aim of monitoring their own remote equipment was highlighted by a number of companies as being a way forward. A major initiative cited in the industrial connectivity domain was the Industrial Internet Consortium. The IIC is a not-for-profit group with an open membership focused on breaking down the barriers of technology silos to support better access to Big Data with improved integration of the physical and digital worlds. The IIC is being led by GE, Oracle and Bosch with Bosch liaising with Industrie 4.0 to provide a connection between the two initiatives. Bosch is promoting the use of OPC-UA within IIC and Industrie 4.0 as an alternative to MQTT. (It should be noted that Bosch has a strong robot technology presence in both the US and EU). The consortium is developing a number of test beds with the aim of creating standards. The testbeds have a steering committee and proprietary projects are performed on interoperability, communications and semantics. Developing standards are promoted through the OMG. It was noted that increasingly companies are realizing that it is not possible to do Big Data handling within companies and there is a need to work with cloud companies. A number of companies see the IIC as a way of accelerating the move towards putting data into cloud companies.

GE are also active in trying to create an industrial operating system PREDEX. This is being promoted for digital industrial businesses as an operating system and platform for building applications that connect to industrial assets, collect and analyse data, and deliver real-time insights for optimising industrial infrastructure and operations. Within this GE uses Wurldtech to provide security.

Machine to machine communication (M2M) is seen as important for product traceability through production processes and it is seen as being interesting for allowing machines to talk back through a chain to other machines to organise production. In the future there will also be a need to consider the link between man and machine and the interactions between the two. However, to support interoperability there is a need for standards for transporting data for M2M and IoT. Already this is being addressed within Industrie 4.0 and US companies highlighted their interest in this, however, it was noted that within this there was a concentration on flexible manufacturing to produce machinery for customised products. More immediately there are opportunities for exploitation of M2M in remote monitoring of machines for on-condition maintenance.

In the area of Fieldbus and wireless connectivity cybersecurity was highlighted as being a major issue. Here it was noted that NIST is leading cybersecurity work in the US and some work was being performed in Industrie 4.0. The NIST Advanced Manufacturing Office (AMO) is leading the National Network for Manufacturing Program and has funded the AMTech program to establish roadmaps and also to fund Manufacturing Innovation Institutes. Here there may be an opportunity to collaborate with Europe.

4.17 Recruitment Sector

At a skills level it was noted that it is difficult to recruit for smart jobs. There are also issues of transferring engineers between the EU and US. If an EU engineer wishes to work in the US there is a need to learn and get US qualifications even though they may have very good European qualifications. This makes the transfer of people and skills difficult. There is also a need to retrain on US standards if engineers are engaged in sectors where different standards apply, e.g. the energy grid sector. Here the harmonization of skills, standards and the process of accreditation would all be beneficial.

4.18 Key Messages and Recommendations from Industry

Smart Cities	
Interested Companies	Of particular interest to large companies – many smaller companies looking for niche applications (e.g. Apps)
Drivers	Green House Gases and Emissions
Barriers	Uncertainty and risk
Challenges	Handling large volumes of data for mobility, sensors, energy awareness
Needs	Need networking technologies, interoperability, spectrum allocation (5G), security, privacy and business models
Automotive	
Interested companies	Large automotive and infrastructure (need interoperability through whole supply chain)
Drivers	Electromobility and autonomous cars
Barriers	Standards for charging stations/connections Autonomous cars - Vienna convention requires driver in control, insurance, liability
Challenges	Siting of charging stations, advising drivers (also to convince can use electric car)
Needs	Big data analysis Global standards for interoperability Need trustable regulation on efficiency and range Fast charging standards and wireless charging

	High resolution mapping and operation in changing/bad weather conditions
Aerospace	
Interested Companies	Large aerospace and small UAV companies
Drivers	Autonomous aircraft and need for skills and competences Monitoring and using data for other applications/services
Barriers	Losing skills Existing regulations demanding pilot in the loop
Challenges	Skilling new generation Large scale deployment of autonomous systems Large scale deployment of monitoring at acceptable cost
Needs	Smart Factories – factories of the future Approaches to educating for skills and competences Model based systems engineering Security of communications
Maritime	
Interested Companies	Ship owners and operators, equipment providers
Drivers	Move to paperless charts and e-Navigation Optimisation of routes Emissions regulations
Barriers	Regulation and lack of standards
Challenges	e-Navigation standards
Needs	Development, testing, validation and verification of new e-Navigation solutions Development and demonstration of route optimisation approaches
Rail	
Interested Companies	Rail operators, Smart Grid manufacturers
Drivers	Electrification and renewal of infrastructure
Barriers	Different standards for hardware, CE, UL and CSA standards

Challenges	Smart Grid linking with renewables
Needs	Harmonisation of standards for Smart Grid
Space	
Interested Companies	Satellite Manufacturers and Service Providers
Drivers	Managing traffic congestion within cities
Barriers	Standards
Challenges	Data management, communications standards, security
Needs	Big data for traffic management, communications and information for autonomous vehicles, surveillance and security
Energy/Smart Grids	
Interested Companies	Large companies and a number of lower tier equipment providers. Large companies set up production in US and Europe to get around certification problems
Drivers	Smart Grids and already companies such as GE are promoting smart platforms for Smart Cities Monitoring of energy efficiency Increased use of renewables, e.g. PV and wind power for car charging
Barriers	Fundamental problems of old infrastructure in the US that needs upgrading Very different approaches adopted in US and Europe Different approaches to standardisation – ANSI in US, IEC for Switchgear and CEN-CENELEC in Europe. The need for UL certification is a major hurdle for EU manufacturers selling to US
Challenges	Renewable sector – lot of competition from China Difficult to introduce new technologies because of existing standards Resistance to unproven technologies.
Needs	Harmonisation of standards Integration of renewables Interoperability - Industrial Internet Consortium seen as very important Telecoms for energy management
Chemical Industry	
Interested Companies	Large chemical plant operators and automation suppliers

Drivers	Plant optimisation for raw resources, energy and water
Barriers	Conservative industry
Challenges	Where to add sensing technology and get payback Many plant workers retiring. Losing skills of how to optimise plant
Needs	Automated systems and optimisation techniques
Automation	
Companies Interested	Automation, sensors, actuator providers
Drivers	Industrie 4.0 Decentralised control and Smart Factories Flexible manufacturing
Barriers	Need to move away from proprietary standards that lock out competition Trade barriers on selling second hand equipment
Challenges	Interoperability for fieldbuses Different wireless standards Data centres - where to locate
Needs	Industrial Internet of Things is seen as way forward via Industrial Internet Consortium Telecommunications and cyber security Harmonisation of wireless standards Regulation for quality of service and reliability OPC UA for the future
Diagnostics	
Companies Interested	Large automation, large information technology and also SMEs
Drivers	Maintenance and predictive maintenance Safety Monitoring Also tracking of components through process (smart tags)
Barriers	Large companies are trying to promote proprietary standards Difficult for smaller companies to get into this market as large corporates

	are preferred.
Challenges	Lack of standardisation How to make money out of data
Needs	Platform standardisation Need standards and protocols for gathering data, e.g. OPC-UA Industrie 4.0 may merge standards which would allow to sell across countries Need security standards IBM is becoming standard for cloud systems
Information Technology	
Companies Interested	Dominated by large companies, SAP, ATOS, IBM
Drivers	Lots of interest in providing cloud for Smart Cities, Smart Transport, Energy, Healthcare, Big Data, IoT, etc.
Barriers	Different national priorities
Challenges	Big Data – Data Privacy, confidentiality Difficult for EU and US to collaborate in area of data
Needs	The need for Governance of data as a product data ownership There is a need for data stewardship and also a need to put into place controls on the purchasing of data OPC-UA is gathering momentum
Wireless Telecoms	
Companies Interested	Large telecoms providers and also SMEs
Drivers	Condition monitoring, maintenance, Smart City, connected car, autonomous driving, smart parking, machine to machine communications in manufacturing, white goods and home automation, Smart Cities, outdoor lighting, video surveillance, waste management substation automation and smart meters
Barriers	Lack of standards for wireless in general Standards for 5G Spectrum allocation for 5G in Europe

	Lack of coordination in area of 5G (particularly in US) Lack of IoT platform for communications Lack of standards for data
Challenges	Interoperability A major hurdle for selling wireless products in US is certification costs Future applications will have millions of devices connected Need battery life of 10 years for end devices Monitoring of battery power of remote sensors
Needs	Harmonisation of technology and standards would be a significant help for small companies There is a need for a 5G standard There is a need for standard data so that it is possible to easily interface different sensors. For the future there is a need for global standards, e.g. Profinet and Ethernet IP There is a need for a standards for white goods interoperability There is a need for a middleware platform and an IoT technology stack that connects components and systems in the field level with the cloud At the machine level the issues of data privacy are not such a concern, however, for personal data there is a need for “Privacy Shield”
Software Development	
Companies Interested	Large software companies and SMEs
Drivers	Support for future IoT and CPS
Barriers	Lack of IoT platform interface standardisation Lack of Embedded Operating Systems standardisation Cybersecurity Differing certification standards
Challenges	Agreement on future IoT platform Cybersecurity Privacy, Safe Harbour
Needs	Funding on IoT and CPS should be directed at use cases building and platform convergence with the aim of creating standards

Research Organisations	
Companies Interested	Non Profit
Drivers	Smart Cities, Smart Grid, Smart Transport
Barriers	Differences in EU and US rules on privacy and personal information Early regulations and standards may stifle innovation
Challenges	Trust will be crucial to exploitation Cybersecurity
Needs	The key technologies of interest are autonomy at rest, autonomy in motion and persistent connectivity There is a need for industrial cybersecurity for IoT/CPS The funding priorities are seen as trust and cyber security There is a need for Data Protection regulation
Standardisation	
Companies Interested	All
Drivers	Interoperability and security
Barriers	Lack of global standards
Challenges	Agreement on key standards
Needs	Industrial connectivity domain - IIC Industrial Internet Consortium Cybersecurity - NIST leading cybersecurity work in the US Industrie 4.0 OPC-UA within IIC and Industrie 4.0 as an alternative to MQQT
Recruitment	
Companies Interested	All
Barriers	If an EU engineer wishes to work in the US there is a need to learn and get US qualifications even though engineers have very good European qualifications
Challenges	Shortage of engineers At a skills level it is difficult to recruit for smart jobs

Needs	Promotion of engineering as a profession Education for smart jobs Agreement on accreditation of qualifications

Table 11. Summary of Key Messages from Interviews

4.20 Summary of Key Recommendations

Smart Cities	6	Need networking technologies, interoperability, spectrum allocation (5G), security, privacy and business models.
Automotive	5	Need Big data analysis, global standards for interoperability, trustable regulation on efficiency and range, fast/wireless charging standards, high resolution mapping to operate in changing/bad weather conditions.
Aerospace	4	Need research into Smart Factories (factories of the future) and need approaches to educating for skills and competences, support for model-based systems engineering and security of communications.
Maritime	2	Need development, testing, validation and verification of new e-Navigation solutions and development and demonstration of route optimisation approaches.
Rail	1	Need harmonisation of standards for Smart Grid.
Space (Traffic Management)	5	Need Big data analysis for traffic management, vehicle-to-infrastructure communications, vehicle-to-vehicle communications for autonomous vehicles, and research in surveillance and security.
Energy/Smart Grid	4	Need harmonisation of standards, integration of renewables, interoperability (Industrial Internet Consortium seen as very important) and telecoms for energy management.
Chemical Industry	2	Autonomous production systems and distributed optimisation techniques.
Automation	6	Industrial Internet of Things is seen as way forward via the Industrial Internet Consortium. There is a need for telecommunications and cyber security, harmonisation of wireless standards and regulation for quality of service/reliability. OPC UA is needed for the future.
Diagnostics	4	Need platform standardisation, standards and protocols for gathering data, e.g. OPC-UA and Industrie 4.0 may merge standards. There is a need for security standards and standards for cloud systems, e.g. IBM is becoming a standard here.
Information Technology	3	There is a need for governance of data considering data ownership and there is a need for data stewardship. There is also a need to put into place controls on the purchasing of data.
Wireless Telecoms	6	The harmonisation of technology and standards would be a significant help for small companies. There is a need for a 5G standard and also standard data so that it is possible to easily interface different sensors. For the future there is a need for global standards, e.g. Profinet and Ethernet IP, and there is a need for a standard for white goods interoperability. A middleware platform is needed and an IoT technology stack that connects components and systems in the field level with the cloud. At the machine level the issues of data privacy are not such a concern, however, for personal data there is a need for “Privacy Shield”.
Software Development	1	Funding on IoT and CPS should be directed at use cases building and platform convergence with the aim of creating standards.

Research Organisations	5	The key technologies of interest are autonomy at rest/motion and persistent connectivity. There is a need for industrial cybersecurity for IoT/CPS, development of trust, and supporting this there is a need for Data Protection regulation.
Standardisation	4	Considering standardisation in the Industrial connectivity domain the IIC Industrial Internet Consortium was highlighted as the way forward. In the area of Cybersecurity the work of NIST was highlighted as the way forward. Industrie 4.0 is seen as the key development in Europe with OPC-UA being promoted within IIC and Industrie 4.0 as an alternative to MQTT.
Recruitment	3	There is a need for the promotion of engineering as a profession and education for smart jobs. There also needs to be agreement on accreditation of qualifications.
Total Number of Key Recommendations	**61**	

Table 12. Summary of Key Recommendations Identified

A summary of the key recommendations identified is shown in Table 12. As found from the analysis of existing programmes the most fertile areas were in Smart Transportation with a total of 12 areas being identified, with Smart Cities being the next most fertile area with 6 areas identified. The area of IoT/CPS is covered by a number of sectors represented notably the Chemical, Automation, Diagnostics, and Information Technology industries plus representation also from other sectors. The technological area of wireless telecommunications was also a fertile area with 6 areas being identified. Overall there is good correlation between the recommendations identified in the analysis of current activities and those highlighted by industry.

In total the interviews highlighted 61 recommendations. Some of these are very specific and also linked with industry priorities, e.g. Industrial Internet Consortium, Industrie 4.0 and OPC-UA. There are, however, some common themes put forward by different industrial sectors in terms of the needs for standards for interoperability of interconnects, wireless communications, protocols and for data exchange. An overriding message was one of the need for data governance, clarity on data ownership and regulation for privacy and the strong need for security. An interesting new area that was highlighted was the shortage of skills and the need to provide proper education for future smart jobs. Here the need for agreement on appropriate accreditations was highlighted to avoid difficulties in movement of personnel or to enable them to work on world-wide products.

5 Views of ETPS, PPPs and Key Clusters

Bio-based economy	Energy	Environment	ICT	Production and processes	Transport
EATIP	Biofuels	WssTP	ARTEMIS	ECTP	ACARE
ETPGAH	EU PV TP		ENIAC	ESTEP	ALICE
FABRE TP	TP OCEAN		EPoSS	EuMaT	ERRAC
Food for Life	RHC		ETP4HPC	FTC	ERTRAC
Forest-based	SmartGrids		euRobotics [AISBL]	Manufuture	Waterborne
Plants	SNETP		NEM	Nanomedicine	
TP Organics	ETIPWind		NESSI	SMR	
	ZEP		Networld 2020	SusChem	
			Photonics 21		

Figure 6. Public Private Partnerships

Significant effort is already on-going in a number of European initiatives (see Figure 6) which have strong engagement from industry and academia. This includes a number of European Technology Platforms (ETPS), Public Private Partnerships (PPPs), and the Knowledge Innovation Centres (KICs) addressing ICT. Additionally clusters of expertise are being created such as AIOTI. To collect the views of these organisations a list was made of relevant bodies which were thought to have an interest in PICASSO outcomes.

The following organisations were contacted: SmartGrids, ENIAC, ECSEL (ARTEMIS-IA, EPoSS and Aeneas were all individually contacted), NESSI, ETP4HPC, Big Data PPP, NEM, Networld2020, ALICE, ACARE, ERRAC, ERTRAC, Waterborne, KIC EIT, EFFRA and AIOTI. Additionally, the views of the Big Data PPP are presented in section 6 in the response from the Big Data Expert Group. Not all of the contacted organisations responded despite significant effort to follow up responses. Responses were, however, obtained from the Networld2020/5G PPP, ETP4HPC, ALICE, AIOTI, with some comment from ARTEMIS-IA, ACARE, NESSI, EFFRA, ERTRAC and Waterborne which resulted in a 56% response rate. It should be noted that in some sectors there is already an interest in EU-US collaboration, however, in other sectors, e.g. Rail (ERTRAC) and Maritime (Waterborne) it was highlighted that it was not immediately clear why EU-US collaboration would be beneficial so it was not possible to respond. Here it was noted that initiatives considering collaboration on surface transport by the TRB–ECTRI Working Group on EU–US Transportation Research Collaboration had previously highlighted a number of issues [2]. EFFRA highlighted that some activities had been supported by IMS (a joint EU-US programme). ACARE highlighted that they primarily addressed European companies and were pursuing the Flightpath 2050 vision and Strategic Research Agenda supporting this. The questionnaire was, however, raised at an ACARE meeting to identify if a response should be made. The ARTEMIS-IA highlighted that it has a focus on EU competitiveness in world markets so it is more difficult to identify where its members may wish to collaborate with the US. In some cases linkages were being made to the application sectors via the applications being considered within the technology driven PPPs, e.g. the 5G PPP which is directly addressing the Automotive, Factories of the Future, eHealth, Energy, Media and Entertainment sectors.

In the following sections the fuller responses received are presented.

5.1 Networld2020/5G PPP

The 5G PPP is concentrating on research and development of 5G communication networks to support new challenging requirements and in 2015 a white paper on the "5G Vision" was published at the Mobile World Congress. The 5G PPP is cooperating with vertical sectors in order to better understand requirements for future networks. This includes the Automotive, Factories of the Future, eHealth, Energy, Media and Entertainment sectors with plans to also investigate other sectors. All of these sectors have relations to Smart Cities. The 5G PPP is interested in understanding the range of technical requirements which are coming from different sectors so that the system design put forward is not limiting for any application domain. The societal drivers come from the application domains and there is interest in supporting mission critical applications (e.g. energy or in general utility systems). The benefits are seen as increasing efficiency of processes in society, economy, administration and industry. An improvement of competitiveness is also expected by bringing manufacturing back to Europe. An increasingly connected society will also improve the life of citizens, will overcome the digital divide and support inclusion. From an industrial perspective improved competitiveness and efficiency are key goals. Security and safety for mission critical applications will be essential for new systems, because many processes and infrastructures are increasingly dependent on ICT. The policy drivers are to support economic growth and job creation in the face of global competition. Here there is a need to develop systems based on globally accepted standards which allow interoperability to open export markets for the European economy. Considering barriers to exploitation, the 5G Manifesto, put forward by leading European network operators and infrastructure vendors, summarised concerns in the regulatory domain. Issues highlighted are availability of sufficient frequency spectrum and the need for net neutrality rules. Standardization for 5G is still mainly being performed in silos so there is a need for enhancement of cooperation between vertical industries and the ICT industry.

The focus of the 5G PPP is obviously 5G, however, there are strong relations to Cloud Computing, Big Data and IoT/CPS. 5G will support three major pillars: enhanced Mobile Broadband (eMBB), massive Machine Type Communication (mMTC) and Ultra Reliable Low Latency Communication (URLLC). These pillars have a clear link to the different technologies. The 5G core network will increasingly use IT elements. Machine type communication is closely related to IoT and CPS. Therefore, there is a need for close cooperation between different technologies.

The main technological issues that need addressing are that the complete network will need to be redesigned. This will require development of radio interface technologies to solve challenging capacity and latency requirements, development of fronthaul and backhaul, new approaches to network management and operation and development of security. There are also implementation issues for high carrier frequency systems and high performance signal processing that need addressing as well as the need to provide spectrum access. Research and development in the area of SDN, NFV, Clouds and Virtualization is needed and the vertical sectors need to be brought together. The main barriers are the regulatory environment and lack of spectrum availability. The funding priorities have already been agreed between the European Commission and the 5G Infrastructure Association within the 5G PPP in the 5G PPP Contractual Arrangement. The private side of the 5G PPP is cooperating with the European Commission to develop the work program where the research priorities are fixed.

Considering EU-US collaboration Horizon 2020 is open for international cooperation and organisations from the US can participate in Horizon 2020 projects. US organisations can participate via subsidiaries in EU Member States, Associated Countries or Candidate Countries and receive funding from the European Commission. If they are based outside these countries they have to organise their own funding. Several companies from the US are already participating in 5G PPP projects via subsidiaries in the EU. In addition, the 5G Infrastructure Association has signed a MoU with 5G Americas (Industry Association) as the representative of the private side on the American continent. This cooperation is used for information exchange and joint events to support consensus building. In addition to collaborative research, there is a lot of cooperation in and between multi-national companies and international standards bodies.

It has to be recognized though that industry is in global competition and no one wants to give up competitive advantages. The US are strong in IT systems and Europe is strong in radio systems and communication networks. In order to bring these worlds together cooperation is needed. On the technology side it is possible to collaborate in all areas. Frequency spectrum is currently handled differently in the US and in Europe. This is where close cooperation is needed. In general there is no area where cooperation should be excluded excepting areas that are in the domain of national security.

5.2 High Performance Computing PPP

The High Performance Computing PPP [3][4] highlighted an interest in Smart Cities, Smart Grid and Smart Transport with an aim of expanding the use of HPC from the more conventional scientific domains to application areas. HPC is seen as an enabling tool and technology which is a ubiquitous tool and method. This is being supported by the ETP4HPC and the related HPC PPP. The societal trend is towards a generalised digitalised society, economy and public services. Additionally, there is an increased demand for safer, cleaner and more efficient technologies and life styles with the need to mitigate the industrial and natural hazards in a more and more populated and connected world. From an industrial perspective large companies like ATOS can deliver high end systems relying on mass market processor and memory components and also IT services around this. Considering the application domains there is interest in the energy sector (including the oil and gas domain), aeronautics and surface transport. There is also interest in the finance and pharmacy sectors. The key topics in HPC are seen as being the exploitation of Big Data and deep learning.

It was noted that IoT may revolutionize business and market segments for HPC and may make it a pervasive technology in many industrial and service areas. The EC defined a global HPC policy in 2012 and recently updated and widened the ambition of this towards the Digital Single Market. The current barriers to exploitation include Intellectual Property ownership for hardware and software. Considering standards, they already exist to a limited extent for HPC software but could be improved with respect to abstractions for hardware and architectures to enable better productivity and sustainability. A very active area at present is business modelling. The ETP4HPC is supporting more pervasive usage of affordable HPC not only at the extreme scale but also at the mid-range and democratised levels. Here it is expected that new business models will be created in the areas of deep learning and Big Data. The key aims in HPC with respect to research are for shorter computation time requiring denser and faster machines with more 'parallel' integration. This will allow more difficult computing or data processing problems to be solved. To achieve this more compute and memory units interconnected by an ultra-fast local network is required. Here there may be a link with 5G in a more and more connected world. One can envisage that in future solutions embedded HPC will be connected to global networks of remotely connected sensors or devices.

The key technological issues and barriers are power efficiency, fault tolerance and reliability of systems that are made from a very high number of components. There are also needs for programmability of highly parallel architectures. The efficiency and sustainability of application software is also a concern regardless of the underlying hardware architecture. The funding priorities are highlighted in the ETP4HPC SRA and the HPC PPP research agenda [5].

It is believed that the EU and US could collaborate on HPC applications, numerical solvers and various math and middleware libraries. Here there are often open source or open API specifications which makes collaboration easier and already the ETP4HPC is supporting and fostering this. An area where it is not possible to collaborate is on hardware development which is strategically, industrially and economically sensitive and locked.

5.3 ALICE

The areas of interest to ALICE (Alliance for Logistics Innovation through Collaboration in Europe) are the Physical Internet [6] [7], Smart Transport, Smart Logistics and Industrie 4.0. The societal trends driving this area are the ageing population, demographic changes, oil price volatility, crowdsourcing and crowd shipping, shared economy, globalization and localization, consumer needs and behaviours and growth of e-commerce. There is also a new Physical Internet paradigm and integration with manufacturing that is changing the landscape with concepts of off and near shoring, cloud manufacturing, etc. These will impact logistics operation and therefore socio-economic aspects such as environment, energy, safety and security, employment and growth.

At an industry level this is being driven by the needs for cost reduction and efficiency and also at a policy level by decarbonisation and environmental policies concentrating on energy consumption reduction and the move towards renewable energies. The current barriers to exploitation are seen as a lack of appropriate business models and the need for a “mind shift” within a sector that is typically traditional and conservative. There is a need to understand the expected impact on the labour force and the required skills for the future. With the increase in automation and digitalisation, workers will have to acquire new skills to exploit new technologies. Already studies in the US, Germany and UK as well as industry statements have highlighted a shortage in truck and locomotive drivers for logistics. The need for education to prepare for demands of the digitalised work environment in order to avoid a widening gap in society between low-skilled and high-skilled workers was emphasised in a World Bank report [8].

The technologies that are of particular interest are robotisation, human machine interfaces, automation of transport and drones, automated delivery vehicles, Internet of Things (IoT), augmented reality, Big Data, Industrie 4.0, 3D printing, machine visualization and learning, 5G and enhanced system interoperability. All of these technologies are likely to have applications within logistics

The key technological issues/barriers that need addressing are to create the ability to rapidly connect to, and disconnect from, supply networks at two levels; the business level and the technical ICT level. There is a need to simplify ICT systems, information interfaces and business models so that domain users are shielded from having to become technology experts and can focus instead on the efficient execution of transport and logistics operations. There is also a need to simplify and standardise the device interconnections so that the rapid connection and disconnection of sensor enabled items is facilitated. On top of this there is a need for Open cloud-based collaboration platforms to facilitate the dynamic and cost effective formation and management of complex supply networks. This will require secure and reliable data management approaches that facilitate the collection and analysis of authorised data so that operational efficiency can be improved while assuring the public that privacy is maintained. Appropriate standards and data collection systems will need to be developed for reporting commercially and socially important information (e.g., emissions, load factors, congestion levels, etc.) so that proper comparisons can be obtained and informed decisions made. There is also a need to create approaches that can properly manage goods flows so that infrastructures, transport assets, modal nodes and other supply network assets are optimally utilised within integrated smart infrastructures and Intelligent Transport Systems (ITSs). These will employ IoT devices and other intelligent edge based technologies in supply chains to increase the efficiency, effectiveness and control of supply networks. These priorities have already been expressed in the ALICE Recommendations for Horizon2020 [9] [10].

As logistics is a global business it is thought that it would be possible for the EU and the US to collaborate on administrative simplification and trade facilitation, standardization and regulation. There is scope for work on modelling and simulation tools and the identification of important parameters and quantitative indicators to describe the logistics system and to assess the socio-economic impact of logistics developments in terms of economy, energy, environment, congestion, infrastructure required, value of transport, employment, education and skills, safety and security, etc. The development, simulation and analysis of scenarios for logistics can contribute to support policies and strategy development within industry, government and all other stakeholders.

5.4 AIOTI

The Alliance on the Internet of Things Innovation (AIOTI) is interested in the areas of Smart Cities, the Smart Grid (considering the “Internet of Energy”) and Smart Mobility (considering multi-modal/autonomous vehicles and also electric mobility). The societal trends that are driving this are global climate change and the change in demographics with a move towards urbanisation and mega districts. In the transportation sector increased electrification of transport and seamless mobility on multi-modal transport systems is driving technology. This includes the need for IoT support for autonomous vehicles but also the use of IoT in vehicle sharing. It was noted that there is a general trend towards “X as a service” in both the energy and mobility markets with the city as a customer. Considering the bigger picture the hyper-connected society will drive the technology. There is a convergence of "Green" technologies, e.g. decarbonising of the grid, transport sectors and cities and a reduction of CO_2 emissions from transport. This requires distributed digital technologies utilising connectivity and data to control a Connected Power Grid which increasingly uses renewable sources. This will lead to the rise of the prosumer. The industrial drivers in the domain are the Internet and the Industrial Internet of Things. There is an increasing use of connected devices requiring communication and network technologies, such as Broadband Wireless (5cG+++), Cloud computing, Edge Computing/Mobile Edge Computing Data processing and the need for improved analytics exploiting cognitive technologies.

The policy drivers for IoT are a transition towards the low-carbon economy and the demand for high security, quality and economic efficiency of supply in a market environment. There is also an increase in consumer empowerment making them more informed, engaged, interested and equipped to play an active role in the market. There is an increase in choice (of suppliers, sources) and the possibility to exercise this choice. In the future there will be increased integration of the energy/mobility/city system environment. Supporting this there are needs for approaches to data handling, privacy and cyber security. Standards are also needed for interoperability. Additionally, regulations and incentives are needed to provide a safe, reliable, sustainable and efficient infrastructure. The current barriers to exploitation are a lack of business models, a lack of interoperability and a lack of harmonisation of national regulations.

The key technological issues/barriers that need addressing are to create the ability to provide reliable electricity to power the billions of IoT devices. In the Internet of Things internet connectivity and power are very important for autonomic edge devices. Accuracy and unambiguity of data will be important for the adoption of IoT considering the amount of data received. The network bandwidth will need to increase to allow tens of billions of devices to be “always” connected to the Internet. Interoperability will also be required to allow easy integration of new devices. Security/trust/privacy are also key requirements. This places demands on legal ownership, storage and sharing of data and the need for end-to-end security frameworks considering security-by-design techniques encompassing software security, embedded security and hardware-encrypted security. The funding priorities for the area are to perform large scale, cross-sectorial deployments of the Internet of Things. Supporting this there is a need for research on cognitive IoT, M2M learning apps and artificial intelligence-based applications. There is also a need for autonomous-based, smart environments and Open data platforms development.

It is believed that it is possible for the EU and US to collaborate on alignment of IoT architecture efforts for the benefit of interoperability of systems from the different domains. There is a need for mapping of IoT reference architectures/platforms showing the direct relationships between elements of the models and a clear roadmap to ensure future interoperability. There is also an opportunity for alignment of requirements for standardisation bodies to influence global standards. Cooperation and collaboration is possible in the area of testbeds and large scale pilots to demonstrate interoperability on the technical and semantic level. It would also be possible to exchange use cases and architectural requirements focused on industrial/business/consumer markets in order to meet the requirements for the different IoT solution implementations. At a higher level it would be useful to align IoT policy frameworks on security, privacy, safety, trust, etc.

5.5 Summary

It is notable that bodies representing the closer to market, application domains, e.g. ARTEMIS-IA, aerospace, maritime, rail, EFFRA, etc. were less able to identify the potential for collaboration. This is constrained by commercial competition and also by differences in regulation within Europe and the US. Despite this initiatives already exist which promote collaboration within a limited context between sectors. Notably there was interest in the application domain of logistics where there are needs for modelling and simulation support to manage complex networks. Here there is a need for fundamental work that addresses problems that are common across a number of stakeholders.

PPPs and organisations addressing fundamental technologies, e.g. 5G, HPC, IoT and Big Data, are very keen to collaborate and highlighted an interest in pursuing joint activities in all areas being addressed by their respective strategic research agendas. However, here there are some areas were identified were it would not be possible to collaborate. These are in the areas of technology where there is direct competition between the EU and US or where there are strategic, industrial or economic implications. Areas that may have implications for national security should also be avoided.

6 Views of the Expert Groups

The views of the three technology driven Expert Groups were canvassed. In this section the views with respect to the Interview Questions are presented.

6.1 IoT/CPS Expert Group View

- **What is/are the application domains that you are interested in, e.g. Smart Cities, Smart Grid, Smart Transport, etc.?**
  - Smart production (smart manufacturing, processing industries)
  - Smart cities
  - Smart grid / smart energy / Internet of Energy
  - Smart mobility / electric mobility / smart transportation
  - Multi-modal / autonomous vehicles
  - Smart logistics
  - Smart buildings
  - Critical infrastructures
  - Healthcare
  - Robotics

- **What do you see as the societal trends that are driving this area?**
  - Global climate change, reduction of greenhouse gas emissions, “green” technologies
  - Decarbonisation of the grid, transport sectors, and cities
  - Clean air and water
  - Renewable energy
  - Digital, distributed, data-controlled, and connected power grids
  - Globalization (and personalization as well)
  - New demographic reality and developments – urbanisation, migration to cities, mega districts, influx of the young population
  - Seamless mobility (multi-modal transport systems, autonomous vehicles, vehicle sharing)
  - Electrification of transport
  - Energy / mobility as a service, the city as a customer
  - Security and safety
  - The hyper-connected society
  - High usage of social media
  - Convergence of technologies
  - The rise of the prosumer

- **What are the industrial drivers for this domain?**
  - The advent of smart and connected devices
  - Communication and network technologies (e.g. broadband wireless, 5G), mobile technologies
  - Internet / Industrial Internet of Things (IIoT) - Systems-of-systems integration applied in industrial environments

- Increased connectivity and autonomy in all application domains
- Cloud computing, (mobile) edge computing, ubiquitous mobile computing
- Advances in data processing and analytics
- Cognitive technologies, advances in AI
- Needs for assurance and cyber-security
- Dependability, resilience
- Demand from both consumers and governments for clean air/water and security/safety, which companies are seeking to satisfy with products and services
- Customer demand is developing for greenhouse gas mitigation
- Predictive maintenance

- **Are there any policy drivers for this domain?**
  - Transition towards the low-carbon economy
  - Security / trust / privacy - legal ownership, storage, and sharing of data. Particularly important for the industrial IoT/CPS systems this EG considers: if data integrity is compromised, the impact will not be on an individual per se, but on the safety and security of the general public in some extended area and of the environment (e.g., disruption of power grids or incidents in chemical plants)
  - Regulations and legal issues in IoT governance
  - Global standardization / certification / interoperability policies as a critical requirement for IoT/CPS
  - Data ownership by multiple providers in the "end-to-end" IoT/CPS data chain: sensor -> comm. network -> cloud -> analytics software -> comm network -> smart actuator (privacy or data protection violation may be impossible to trace back to the offending party)
  - Legal issues regarding the potential supervision of workers, operators, private citizens
  - Safe, reliable, sustainable, and efficient infrastructures
  - High security, quality, and economic efficiency of supply in a market environment
  - Consumer empowerment
    - Informed and engaged, i.e. interested and equipped to play an active role in the market
    - Provided with choice (of suppliers, sources) and the possibility to exercise the choice
    - Integrated in energy / mobility / city system environment
  - Public-private partnerships
  - Policies to build a strong innovation ecosystem (start-ups, student incubators must be able to exchange ideas and collaborate, co-develop)

- **Are there any current barriers to exploitation, e.g. regulations, lack of standards, lack of business models?**
  - Differences in national priorities, rules, and regulations, e.g. on privacy and personal information
  - Security, safety, privacy concerns: Heterogeneity of attack points with lack of end-to-end standards; safety-relevant areas
  - Lack of interoperability and (device) standards: A large variety of proprietary interfaces, protocols, and data formats exists, and nominally following the same standard will often not achieve interoperability
  - Lack of trust (would be detrimental to exploitation)
  - Barriers for cost-effective and clean solutions: The fact that externalities such as the CO2 footprint of conventional systems are not factored into prices is a major barrier to developing cost-effective and clean alternatives - this complicates the challenge of devising effective business models
  - Lack of business models
  - Restrictions on foreign partner funding
  - Export control
  - Lack of skills: Lack of trained specialists for data intake, data scientists, security experts, network experts

- **What are the technologies that you are particularly interested in, e.g. 5G, Big Data, IoT/CPS?**
  - Internet of Things
  - Cyber-physical systems
  - Autonomy
  - Cyber-security

- Cognition / artificial intelligence / situational awareness
- Big Data analytics, data-based operation
- (Mobile) communication and network technologies, persistent connectivity
- Interoperability, integration, reconfiguration
- Pervasive sensing
- Strong need for support of humans, humans in the loop
- System-wide optimization
- Heterogeneous models of cyber-physical systems, model integration, model management
- Platforms

- **In your opinion what are the key technological issues/barriers that need addressing?**
  - **Closed-loop IoT/CPS systems:** How can the huge amounts of real-time data produced by IoT-connected sensors be transformed into useful knowledge and actions?
  - **Autonomy in open systems:** Large-scale complex systems are not domain/knowledge-"contained". How can we enable autonomy beyond highly circumscribed areas (using e.g. world models)?
  - **Cyber-security / end-to-end security frameworks**: Security of IoT/CPS systems is an important research priority. We can build just about anything that we set our minds on, but whether we build it correctly, accounting for all of the attack vectors introduced into those systems is another matter. More research is needed on engineering sufficient security into all systems that are built, not adding it on at the end. Thus, security-by-design techniques are needed that consider software security, embedded security, and hardware-encrypted security, and that enable data protection and privacy.
  - **Interoperability and integration**
  - **New approaches to handle uncertainty and risk**
  - **Heterogeneous modelling:** Models of cyber-physical systems, model integration, model management, verification of models developed from large volumes of data
  - **Sensing technology:** Scalability of sensors (making sensors smaller), size of sensor memory, in-memory computing power, cost/benefit ratio of sensors (making sensors less expensive and affordable), speed of data exchange between sensors and the internet
  - **Reliable electricity to power the billions of IoT devices:** This is a challenge, as IoT is becoming a dominant market consideration, and two functions (internet connectivity and power) are very important for autonomic edge devices
  - **Being always-connected:** The network bandwidth needed for connecting tens of billions of devices to the internet the need to be "always" connected
  - **Accuracy and unambiguity of data** is an important element in the adoption of IoT and its use to close the loop in CPS, considering the amount of data received

- **What in your opinion are the funding priorities for this area?**
  - In the US, the National Science Foundation has a major initiative in CPS - energy aspects are of particular interest
  - Internet of Things: Large-scale cross-sectorial deployments as part of overall digital strategy
  - Cognitive IoT, M2M learning apps, and artificial intelligence-based applications
  - Autonomy-based smart environments
  - Development of open data platforms
  - Big Data analytics, sharing of data with privacy provisions

- **Where do you believe it is possible for the EU and US to collaborate?**
  - There is an opportunity to collaborate in addressing the challenges of energy, air, and water in poorer parts of the world (e.g., Africa, China, India and Latin America). Within this space, commercial opportunities may be limited in the near term, so competitive conflicts are less likely. Yet these problems need to be resolved and we will ultimately all be worse off, including in developed economies, if they are not resolved.
  - Fundamental research (not too close to immediate commercial interests)
  - Interoperability, harmonization of standards

- Policy discussions
- Alignment of IoT architecture efforts for the benefit of interoperability of systems from the different domains
- Mapping of IoT reference architectures/platforms showing the direct relationships between elements of the models and a clear roadmap to ensure future interoperability
- Alignment of requirements for standardization bodies to influence global standards
- Cooperation and collaboration in the areas of testbeds, and large-scale pilots that will ensure interoperability on the technical and semantic level
- Exchange use cases and architectural requirements focused on industrial/business/consumer markets in order to meet the requirements in its specification for the different IoT solution implementations
- Alignment of IoT policy frameworks on security, privacy, safety, trust etc.

- **Where do you think it is not possible for the EU and US to collaborate?**
  - Products and services that may lead to large profitable businesses in the near term / areas of high near-term commercial importance
  - Joint funding (funds will not cross the Atlantic)
  - Aspects relating to export control issues
  - In the areas where classified information or data is necessary
  - Areas where data privacy and security questions become sensitive and local legal obstacles may be very cumbersome to overcome

6.2 5G Expert Group View

- **What is/are the application domains that you are interested in, e.g. Smart Cities, Smart Grid, Smart Transport, etc.?**
  - Vertical Industries
    - Automotive & Agriculture
    - Industrie 4.0/ Manufacturing/ Robotics
    - Health / Wellbeing
    - Energy
    - Media & Entertainment
  - Emerging applications
    - Fashion design & Sales
    - Edutainment (Learning/ Teaching)
    - Sports (Training & Spectators)
    - Logistics with drones

- **What do you see as the societal trends that are driving this area?**
  - Demographic change, Health, and wellbeing;
  - Secure, clean and efficient energy;
  - Smart, green and integrated transport;
  - Environment, and resource efficiency;
  - Secure societies - protecting freedom and security of Europe and its citizens;
  - Europe in a changing world - inclusive, innovative and reflective societies;
  - User centric information User centric networks, user centric X.

- **What are the industrial drivers for this domain?**
  - Integration with vertical industries
  - New business models

- Improved operational efficiency and thus reduced cost
- Improved customer experience and satisfaction
- Globally harmonized spectrum
- Virtualisation

- **Are there any policy drivers for this domain?**
  - Network Neutrality / Dedicated network access and control for mission critical vs. non critical services
  - Globally harmonized spectrum
  - Flexible regulatory framework/ spectrum access policies
  - Global technology standard
  - Privacy control – Data ownership
  - Geographic coverage both in country and world wide
  - Framework for new business creation

- **Are there any current barriers to exploitation, e.g. regulations, lack of standards, lack of business models?**
  - High entry barriers for new businesses
  - Business case for initial low penetration / gradual roll-out
  - Fragmented spectrum allocation
  - Different spectrum access policies
  - Lack of interoperability (e.g. btw. IEEE & 3GPP standards)
  - Fragmented regulations on privacy, data ownership and security
  - Liability –when things don't work
  - Regulation for increasingly autonomous things

- **What are the technologies that you are particularly interested in, e.g. 5G, Big Data, IoT/CPS?**
  - mmWave Antenna / Massive MIMO technology - to improve data rates and capacity resp.
  - Spatial Spectrum Mgmt – to overcome scarce radio resource utilisation
  - Improved Network slicing - to meet different service requirements
  - Access technology for XXL cells - to enable coverage in sparsely populated areas
  - Enhanced Network & Device management - to enable Massive IoT

- **In your opinion what are the key technological issues/barriers that need addressing?**
  - Low latency
  - High reliability
  - Massive MIMO
  - System Integration
  - Spectrum Management Techniques
  - Prototyping and testing to verify:
    - Interoperability
    - Coexistence
    - Power consumption
    - Data capacity
    - etc.

    as a complete infrastructure

- **What in your opinion are the funding priorities for this area?**
  - Focus on 5G technologies and applications with market entry beyond 2025

- **Where do you believe it is possible for the EU and US to collaborate?**
  - Both EU and US have a proven R&D capabilities in
    - mmWave channel sounding and modelling
    - Massive MIMO
    - Spectrum Management Techniques
    - Prototyping and testing

- **Where do you think it is not possible for the EU and US to collaborate?**

- Due to the fact that frequency regulation is handled on the national level in the EU, it might become difficult to collaborate with US on this topic.
- Regarding privacy and data protection may face some challenging policy and organizational obstacles.
- Industry policy: it might be helpful to exchange ideas, but a collaboration seems difficult.

6.3 Big Data Expert Group View

- **What is/are the application domains that you are interested in, e.g. Smart Cities, Smart Grid, Smart Transport, etc.?**
  - Smart Transport
  - Mobility
  - Logistics
  - Smart Cities
  - Industrie 4.0

- **What do you see as the societal trends that are driving this area?**
  - Reduction of emissions
  - Reduction of (fatal) accidents on the road
  - Increasing heterogeneous, distributed data ownership
  - Increased specialization, requiring more data and information sharing and exchange
  - Increased awareness of data being a resource or commodity

- **What are the industrial drivers for this domain?**
  - Improved operational efficiency and thus reduced cost
  - Improved customer experience and satisfaction
  - New business models
  - Data is increasingly seen as a key asset, resource and commodity by the industry
  - Digitization of businesses requires proper data management and governance strategies responding to the heterogeneous, distributed nature of the data

- **Are there any policy drivers for this domain?**
  - Reduction of (fatal) accidents on the road
  - Better use of transportation assets
  - European digital single market (more efficient and affordable parcel delivery)
  - Policies should require to make open government data available in machine readable (preferably semantics preserving formats)
  - Users should be granted the right (by law) to obtain all their personal data stored by internet/web portals/services in machine readable (preferably semantics preserving formats)

- **Are there any current barriers to exploitation, e.g. regulations, lack of standards, lack of business models?**
  - Data protection concerns
  - Data sharing concerns across multi-stakeholder supply chains
  - Data collection concerns (cost and effort of data collection vs. value that can be derived from data)
  - Data is often locked in proprietary services and open data is often not available in machine-readable semantics preserving formats
  - Standards should be accompanied by machine-readable and semantics-preserving representations of the content (e.g. as RDF-S vocabularies), so that their implementation is more efficient and effective

- **What are the technologies that you are particularly interested in, e.g. 5G, Big Data, IoT/CPS?**
    - Big Data
    - Semantic Technologies
    - Knowledge Graphs
    - Semantic Data Lakes
    - Data Value Chains
    - Data Spaces

- **In your opinion what are the key technological issues/barriers that need addressing?**
    - **Software architectures and languages for big data.** Apart from large, long-standing batch jobs, many big data queries involve small, short and increasingly interactive jobs. What kind of new architectures (or languages) are required for these new environments? Also, as data protection concerns of data-intensive software systems increase, how can we exploit advances in secure hardware and cryptography to deliver trusted big data systems?
    - **Quality assurance for big data software.** How can we ensure the quality of big data software through adopting and extending proven quality assurance techniques from software engineering? Can we generate (for instance by means of simulation) sufficient and representative test data (e.g., covering extreme cases) in order to ensure resilience and robustness of big data applications? Can we complement testing with (formal) verification techniques for big data? How can we leverage fast prototyping to test the quality of big data applications early on during development; e.g., by using interpreted languages for fast feature deployment and debugging? How can we monitor and thus ensure the quality of big data systems during their operation?
    - **Big data engineering methods and frameworks.** How can we support the engineering of big data applications through targeted methods and platforms? How can we pave the way from online analytical processing (OLAP) systems to full-fledged big data analysis frameworks that bring big data technology into a systems perspective?
    - **Technologies for establishing (industrial) data spaces** including strategies for heterogeneous data evolution, governance, interlinking, analytics

- **What in your opinion are the funding priorities for this area?**
    - Mature, proven and empirically sound engineering approaches and methodologies for building next generation Big Data systems that leverage existing Big Data technologies and tools

- **Where do you believe it is possible for the EU and US to collaborate?**
    - Both EU and US have a strong record on Big Data tools; adding the layer of engineering methodologies would provide a common umbrella for advancing the way we build Big Data systems

- **Where do you think it is not possible for the EU and US to collaborate?**
    - Due to the very specific requirements imposed by the EU federative system, several of the Digital Single Market aspects may not be relevant from a US point of view.
    - Regarding Data Protection, collaboration would be very much appreciated but may face some challenging policy and organizational obstacles.

7 Policy Issues

One of the objectives of the PICASSO project is to bring forward policy recommendations that are designed to improve EU-US ICT collaboration. When talking with the Policy Expert Group members there is clear convergence towards a core set of policy issues that is touching upon all three PICASSO technical domains, and it is generally recognised that these policy issues raise both challenges and opportunities to ICT collaboration. The group of experts that has contributed to this view covers different “stakes” in society, ranging from technical community, to business, civil society and public policy.

During the first meeting PICASSO meeting on 20 May 2016 in Washington DC, hosted by NIST at the Department of Commerce, PICASSO experts and other experts focused on identifying key issues in each focus technology area (5G, Big Data, IoT/CPS) and on those policy issues that influence and are influenced by all of these domains. The responses during individual conversations were also brought into the expert working group discussions, and there was a strong convergence in the issues identified. Considering the input from the three specific PICASSO domains on 5G Networks, Big Data, and Cyber-Physical Systems/Internet of Things as obtained in the context of earlier PICASSO preparatory project meetings the following list of the most relevant cross-cutting policy issues in EU-US ICT collaboration were highlighted:

1. Privacy and Data Protection issues;
2. Security issues;
3. Standardization issues; and
4. Spectrum issues

It was recognized that all these issues bring both opportunities and barriers to EU-US ICT collaboration, and this was explored in conversations. Obviously, the impact varies per PICASSO domain, both in nature and priority. This is also expressed in the summaries per policy issue provided below.

7.1 Privacy and Data Protection Issues

One of the most contested issues across the board is Data Protection of natural persons and their privacy. This is not only a matter of concern to private sector and civil society stakeholders, but is also an increasing bone of contention between national and supranational governments in relation to criminal justice, national security and other vital national interests.

All people interviewed recognised that these issues are entangled with all PICASSO-related ICT developments across the Atlantic, directly affecting ICT collaboration. Whereas technology can help addressing policy/societal challenges in ways that have not been possible before, it also poses new challenges for policy/society that need to be considered. In particular, the real and perceived policy differences between the EU and USA may make it more difficult for ICT researchers to collaborate towards technology and technology deployment solutions that are suitable for both US and EU markets. In this there is a role for commerce, business and the economy, since economic methods and motives drive both policy and technology, as well as provide their own forms of problems and solutions.

In addition to being an important topic in its own right, privacy and data protection issues complicate trade negotiations, freedom of information rules, digital rights, intellectual property protection and financial regulation. With particular reference to the transatlantic dimension and the specific PICASSO domains of 5G networks, Big Data, and IoT/CPS, it features in the evolving arrangements over corporations’ personal data collection, storage, processing and access (on one side the EU-US Privacy Shield, which tends to restrain businesses, and on the other those provisions in TTIP, TPP and especially TSIA that effectively protect corporations from government restraint).

Beyond this direct consideration of transatlantic data flows are indirect tensions arising from divergent legislative and legal developments. A framework for collaboration needs to fully reflect the shared democratic and individual rights-based values, which are expressed on the EU side in the Lisbon Treaty and the Charter of Fundamental Rights, and on the US side by the US Constitution. Dealing with these issues in a collaborative way is difficult, as personal data protection is considered a fundamental right under EU law, and an economic right under US law.

Whereas the draft *Privacy Shield* which is under development to replace the *Safe Harbour* agreement that was dismissed by the European Court of Justice may be a step in the right direction, it is still under discussion as some parties feel it may not adequately include appropriate safeguards to protect the EU rights of the individual to privacy and data protection also with regard to judicial redress and thus may be subject to a negative ECJ ruling, as its predecessor. Furthermore, *Privacy Shield* is created this year, while knowing that from May 2018 onwards new legislation will be in place in Europe. Hence the validity under the current legal framework may need adaption by that time.

In the discussion, it was argued that privacy and interoperability of systems are two sides of the same coin, both being important. Participants agreed that it would be important for industry to explicitly consider the human element from the outset when developing industrial solutions to ensure interoperability and empower services with data streams.

Towards policy decision makers and citizens/consumers, there is a call for awareness raising. It would be important to provide better insight in what operational level technologies can do, and do, today. It was concluded that there is often limited insight in what is happening on the ground.

Specifically for the three PICASSO domains impact of Privacy and data protection can be summarised as presented in the next sections.

7.1.1 5G

In our move towards a hyper-connected society, 5G networks are likely to play a major role. Building on the 4G achievements 5G networks will also facilitate massive amounts of sensors, both mobile and fixed, using relatively little energy, and ultra-reliable communications that can serve as (very) remote controls. Following full implementation of 5G the world is ready to further tag, track and trace any object that is substantial enough for you to want to know where it is, from bikes to computers to basically any gadgets over 50 USD/EUR in purchase. Through the ability to be connected everywhere, all the time, including location tagging, additional masses of data become available that may be related to natural persons, if not directly, then through the use of other data and algorithms.

The danger is that through this it will become possible to track, trace and relate to natural persons which would lead to privacy infringements that go well beyond anything we have seen today. This is already possible today, yet connectivity networks are still relatively patchy and it is costly to do. With networks becoming more ubiquitous and the costs of additional tracking and tracing going down dramatically, regulation will be needed to avoid businesses (and governments) from infringing privacy. A question is whether there is a need for self-regulation, or regulation via international and national law. A first step will be raising awareness among citizens, consumers and policy makers of the potential effects, and to start a multi-stakeholder dialogue of how to deal with this. Core in this is access and use of data, either by persons or machines/algorithms.

The opportunity for EU-US collaboration is in development of systems in such a way that location and exchange of data are transparent to those that are in the system, and that alternatives are available. In addition, a code of ethics could be developed that determines the limits of data gathering and combination, balancing societal and commercial interests with the privacy and data protection principles that are considered a fundamental right in Europe. A particular issue is the need for algorithms that can act "ethically" (respecting fundamental rights).

7.1.2 Big Data

With the connection between data through communication networks it has become possible to access and relate masses of data, potentially to a fine detail relating to private individuals. The ability to combine masses of data comes not only with this threat, but also with the promise of new ways to be able to effectively deal with societal challenges, and business challenges.

Challenges will be to create new services within the boundaries of the Law that currently (in Europe) disallow use of personal data for other purposes than those that were indicated when collecting them. In particular, this limitation would keep developers from the EU back in a global market where others (who are not using European citizen's data) have much more room for manoeuvring.

Opportunities will be in creating ecosystems that are trusted and that comply with data protection legislation, providing services that private individuals want and are consenting to. By creating such services that both comply with US and EU law a product is developed that can have global impact.

7.1.3 Cyber Physical Systems / Internet of Things

Within PICASSO the focus is specifically on large-scale systems, and industrial and closed-loop systems that connect to physical actuators, including safety-critical applications. Most of these will be business-to-business and overall with less relevance to private individuals than the IoT domain at large. It is noted that the result of compromising data integrity may go well beyond privacy infringements and may go at cost of public safety and security, and environmental safety.

A specific challenge in CPS/IoT environments is that data ownership and control may pass through multiple actors, and that information that could relate to private individuals may also be relevant to keep systems safe and secure. In EU-US collaboration the limitations in this are more stringent under European legislation (which includes privacy as a fundamental right) than under US legislation.

The opportunity here is similar to the Big Data opportunity by creating CPS/IoT ecosystems that are trusted and complying with data protection legislation, providing services that private individuals want and are consenting to. By creating such services that both comply with US and EU law a product is developed that can have global impact.

7.2 Security issues

With the increased criticality of connections, connected systems and shared data streams for our society our dependability increases as well. The networks today have not been developed to deal with such challenges and this leads to serious concerns. Without security we have “nothing” we can depend on; so ensuring a certain level of security will be a key requirement for all ICT applications developed in the EU/US. This was widely recognized by all involved, and it affects all three PICASSO areas in similar ways.

The challenge for collaboration in each of the three domains is that there are specific legislative requirements for some applications depending on jurisdiction and application. There is no “general reference law” on either side of the Atlantic and businesses are expected to deal with security issues in a responsible way.

The opportunity is twofold:

1- Setting up a clear taxonomy on security (and safety) sensitivity of specific applications will allow to distinguish those areas where additional effort is needed from those that are less sensitive to the challenges;
2- By developing (more) secure systems that comply with the requirements from both US and EU legislation and expectations, ICT developers will develop products and services that have a clear global market advantage.

7.3 Standards issues

Standards are important to ensure interoperability, but also relate to possible antitrust issues, in particular in EU-US trade considerations. ICT related standards today are mostly developing on a global level, often beyond the traditional standards bodies that were very sectoral and now rapidly converging. Global standards avoid regional trade challenges while at the same time making sure global standards comply with standards from specific regions may lead to a favourable market position for businesses from those regions. Setting global standards thus becomes a commercial issue.

Standards also reflect requirements from legislator nature and thus setting standards, and in particular global standards, becomes a regional policy concern. This affects all three PICASSO domains equally.

In this there is the specific issue of open standards that can help prevent lock-in and emergence of new of technologies and services that are interoperable from the outset.

The challenge is to find a way to operate in a new global economy where many ICT products are applied in multiple sectors. Thus the old ways of setting standards no longer serves as they used to do.

The opportunity is in working together to develop (open) standards that serve both European and American markets, and thus global markets. The sheer size of the market will have an important influence on standards adopted in other regions.

7.4 Spectrum issues

For both 5G and IoT/CPS, spectrum issues arise in particular because of the differences that historically exist on spectrum policies around the world. Whereas spectrum issues as such have been limiting but have been dealt with, spectrum is likely to be used more and more, and the fact that spectrum is so dispersed around the world places high importance on addressing this issue to avoid running into dead-end solutions. It is clear is that some solutions will not be scalable in the long run. The challenge is that spectrum issues vary around the world, and that increasing numbers of devices will make use of more and more of the available bandwidth which requires greater care about the use of bandwidth.

The opportunity is to find EU/US solutions that may not only serve sustainability of overall spectrum use in the long run but may also affect use of energy (i.e. frequency of communications with a better fit to need, etc.)

In general, EU/US collaboration would benefit from the following principles in the set-up of systems thus to better serve markets (trust in technologies and networks) and ability to interconnect.

- Transparency: to make people understand what the environment they are in does with respect to data and privacy, e.g. disclosure (opt-in and user control where possible), (publicly stated/disclosed) fair use where needed; enforceable disclosure, and also provide data ownership clarity.
- Accountability: needed for enforceability, liability, etc., with built-in, self-enforcing mechanisms that keep actors from inflicting damage on others
- Context: so that consumers are not surprised. This requires interoperability, security, standards, etc.

Here two suggestions were put forward:

- A practical proposal for action would be to develop a taxonomy for "privacy sensitivity", "security", and "safety" of different categories of 5G/IoT/Big Data applications
- Develop a good practice framework that can be used to illustrate what is needed.

There was also a suggestion to consider "smart cities" as an application example as this would bring all these issues together to truly deploy new technologies in ways where they are directly confronted with citizens' expectations and wishes and with administrations whose aim is to serve in the best possible way.

8 Barriers

Throughout the report a number of barriers are highlighted. The analysis of ongoing activities highlighted a number of barriers in terms of the need for harmonisation of regulations and standards. This was echoed by the industry interviews which gave more specific detail on standards (in particular the use of proprietary standards) and also highlighted additional practical barriers such as different infrastructure (e.g. energy industry), different cultural approaches, the need to address liability, uncertainty/risk and lack of skills. Notably at the research level the PPPs, ETPs etc. saw fewer barriers but identified the need to avoid areas where there was clear competition and the need to address harmonisation of regulations and standards to remove these obstacles.

The responses of the 5G, Big Data, CPS/IoT and Policy Expert Groups in the previous section clearly outline the considered views of the groups with respect to the key barriers which need addressing within the PICASSO technology and policy domains. In this section the overriding barriers that were highlighted with respect to the societal domains (Smart Cities, Smart Transportation and Smart Grid) being considered within PICASSO are brought together and summarised. Here it is notable that there are some very similar issues across domains which, if addressed, would have impact in multiple sectors. Finally, the industry interviews also highlighted some cultural business differences between EU and US companies that can also be considered to be potential barriers to collaboration. These are presented in section 8.4.

8.1 Smart Cities

In the area of Smart Cities a number of barriers to exploitation of new technologies were identified. It is noticeable that although there are many case studies around the world which show the application of smart technologies there is still no fully integrated Smart City that demonstrates the benefits of such an integrated system. As a result, there is no reliable information available for cities or service providers on the costs and potential benefits from adopting smart technologies or the difficulties associated with implementation. The following barriers exist:

Lack of a Vision and an Innovation Culture: City government tends to lack a clear vision or innovative attitude.

Lack of Integration: Some of the benefits of Smart Cities will only become apparent once systems have been fully integrated.

Demonstration at Scale: The larger the number of participants on a particular system, the greater the benefits to all users. However, the scale of the investment and the complexity of linking up networks and organisations to develop a Smart City system presents a co-ordination challenge.

Risk: City Authorities need to take a lead but there are risks which naturally result in caution. They are thus more likely to be "followers" rather than leaders when it comes to exploiting technologies. City Authorities are also more likely to want to learn from others' experience.

Financial Constraints: City leaders are under financial constraints.

Investment Rules: Funding for investment and procurement rules may inhibit innovation. In the US, pilots and demonstrators to develop new innovative approaches for public service delivery are able to access private capital. Within Europe cities tend to rely on Government programmes in specific areas, e.g. Smart Grids or intelligent transport.

Business Models: While the attraction of citizen-centric service models are clear, the business models to support services supplied in partnership with the private sector need to be developed.

Inclusivity of Public Services: Local authorities are keen to maintain inclusivity of their services and ensure that all citizens can embrace new forms of delivery.

Fear of Lock-In: There are concerns about proprietary business lock-in in relation to smart applications and systems. This is reinforced through network effects, as more service systems join the same network the cost of changing to a new system becomes prohibitive. Ensuring the interoperability of systems through open standards is considered essential in order to remove such concerns and enable new approaches to be adopted across the EU and in global markets.

Data-use Legislation and Security: Here there is a need to tackle the issue of ownership of data. There is also a need to address trust in data privacy and system integrity. More highly networked systems, and exchange of data between networks, will inevitably share more data about users. Increased interconnectivity between systems also leads to increased vulnerability to deliberate disruption by malicious actors. Here there are concerns about the risks of access to data either for unauthorised use, threat of criminal access to systems, or a breach of an individuals' privacy. For operators of systems and users there is a need to provide suitably rigorous approaches that insure that the information which is collected, stored and transmitted is secure. There is a need for good implementation of cyber security and also clear communication with service users about how data about them is used and protected in order to build trust. For acceptance there is also a need to demonstrate how the use of their data benefits them.

8.2 Smart Transportation

In the area of Smart Transportation there are already many initiatives looking at Intelligent Traffic Management to reduce emissions and here the problem is one of providing sensors to gather information and information to drivers to reduce congestion. The key area where critical barriers exist is in the area of autonomous vehicles. Manufacturers believe that autonomous driving is an important technology to make road traffic more secure and more efficient. The move to greater automation and eventually driverless vehicles is very much the current Zeitgeist and the whole industry is trying to move in this direction. An increasing number of driverless cars are being deployed within constrained settings and Advanced Driver Assist Systems (ADAS) are already being sold. As it is still early days for autonomous cars there is no reliable information available to cities or service providers on the costs and potential benefits from Smart Transportation, or the difficulties associated with implementation. The following barriers exist:

Lack of Supporting Infrastructure: The industry has been working for 10-15 years already on car-to-infrastructure and car-to-car communications. The key need here is world-wide standards that cover Europe, American, Japan and China. Considering communication with infrastructure there is a need to provide appropriate supporting technology. In the US a standard for short-range communications using IEEE 802.11 protocols is being promoted by the Intelligent Transportation Society of America and the United States Department of Transportation, however, a global standard is needed. Work is also needed on longer range communications standards. The industry view is that communication between cars and infrastructure is the future but there is a need for experience from day-one applications. There are a number of barriers to adoption including the difficulty of integrating with legacy equipment, justifying the need for investment to government and the slow and bureaucratic decision making process of government.

Demonstration at Scale: The majority of the work is on quite low level technical solutions, e.g. processor architectures, sensor technologies, data processing algorithms, but little is being done about how a population of such vehicles, mixed with more traditional vehicles, will actually behave, especially under fault conditions. It is unrealistic to assume that the designers will be able to anticipate all possible eventualities and put in place necessary and sufficient mitigations. Although a few autonomous cars have been demonstrated the true benefits of autonomous driving will not be realised until there are a significant number of cars on the roads. With sufficient autonomous cars there will be an effect on the overall traffic flow. At this point many of the predicted benefits with respect to fuel economy and emissions will be realised. The expectation is that even if only a few cars are equipped with the technology, e.g. 2-3%, then their modified behaviour will affect all other cars.

Liability: Risk of an accident is a huge concern for the automotive industry. The implications of this are just being realized with the recent crashes of the Tesla car, one of which resulted in a fatality. There is a need to understand liability and provide clear guidance in this area. Already Tesla has changed the name of their autonomous driving system to an Advanced Driver Assist System to ensure that it is clear that the driver is the ultimate responsibility in the case of an accident. Another key issue for autonomous cars is risk. Accidents are inevitable and what process is adopted when accidents happen is important. Here there are issues of how is responsibility apportioned among a myriad of suppliers and sub-suppliers and what do victims have to do to get support for their loss and/or recovery , i.e. they should not need to battle through the courts for 10 years.

Financial Constraints: From the perspective of automotive manufacturers cost is a key factor. The addition of sensors and functionality to provide autonomous driving needs to be at a level that customers are prepared to pay for. Cost has been a factor in the slow uptake of electric cars but this is now being addressed as batteries are produced more cheaply. For autonomous cars it will be a number of years before the costs can be reduced such that the technology can be applied to lower end models. At the smart infrastructure level there is a need for very expensive infrastructure deployment. It should be noted that a key requirement in any infrastructure implementation is the ability to be future proof and allow for future likely innovations. This is challenging as electronics typically becomes obsolescent in 18 months and a car in 10 years. An infrastructure investment needs to last 30 years or more and to operate the system requires built-in functionality for remote monitoring to allow for maintenance.

Business Models: New business models need to be developed and these may also have social implications. Current conflicts in France between Uber and taxi drivers show that the development of new transport services and business models may not be compatible with the old ways of organising things. In order to provide future services all the PICASSO technologies need to come together. CPS is needed to provide autonomous vehicles, 5G is needed to provide high data rate communications to connect mobile users to servers providing data. Big Data is needed to collect information on traffic status and transport needs, and IoT is needed to connect sensors for monitoring traffic. Here a number of business models will need to be connected together.

Legislation for Safety: Although increased autonomy is the future there are still technical and legislative hurdles that need to be addressed before a 100% autonomous car is possible. Across Europe there are many different national regulations for safety that need to be harmonised to allow cars to be operated. Notably there are fewer barriers to implementation in the USA. Here public perception and trust is a major barrier at present.

Data-use Legislation: There is a need for intensive real time monitoring of the performance of the systems to spot potential issues arising before they develop into accidents. This raises concerns over privacy. There are needs for protection from unscrupulous companies and state surveillance, and also security to provide protection from criminals and terrorists. The issue of data privacy is something that needs to be addressed at the European level as different countries have different views on privacy with different regulatory and political interests. For instance, at a political level in Germany privacy is a very important topic and technology cannot be used for tracking cars. In France there is a different point of view and so car tracking is also possible. There is also a need to build trust and to clearly explain to users how their data is being used to benefit them.

Risk of Disruption: Increased interconnectivity between systems leads to increased vulnerability to deliberate disruption by malicious actors. For operators of systems and users there is a need to have in place rigorous cyber security to ensure that the information which is collected, stored and transmitted is secure.

8.3 Smart Energy and Smart Grid

A challenge in the Smart Energy and Smart Grid area is that around the world very different implementation approaches are being adopted. National and regional business drivers are resulting in a number of technologies and services being demonstrated. There are also fundamentally different business approaches being adopted. In the US peak load reduction technology and dynamic pricing tariffs are being pursued whereas different approaches are being adopted in Europe. There is also a major push towards the integration of renewables which is changing the energy landscape. Here there is strong competition from China.

Need to Integrate with Existing Infrastructure: Any new grid technology needs to be integrated with the existing infrastructure. In the US there is considerable investment in upgrading old out of date infrastructure. In Europe the infrastructure is far newer. Notably the integration of renewable technologies requires significant changes to existing infrastructure.

Resistance to New Technologies: There is a resistance to unproven technologies in the industry. This makes it very difficult to propose and test new technologies in the grid. Without the opportunity to test new technologies it is not possible to prove them. Thus there is a circular problem. Existing standards are also prescriptive and in many cases prevent new technologies being adopted.

Wide Deviation in EU and US Standards: Europe and the US use different voltage levels and frequencies. Different standards have evolved on both sides of the Atlantic and there are also different approaches to standardisation with ANSI in US and CEN-CENELEC in Europe. Already this presents barriers for selling equipment from European manufacturers to the US and vice versa.

Financial Constraints: It is very expensive to introduce new energy infrastructure. Already major programmes are underway in the EU and the US but much of the work on Smart Grid is being financed by the energy companies themselves. This leads to caution in terms of roll out of technologies. The opportunities for smaller companies (where innovation is more likely to evolve) to engage in the sector are more limited.

Data-use Legislation: There are some issues with the collection of energy use information and the privacy of this data but this is less sensitive than other areas. Already smart meters are widely deployed and customers can be easily persuaded of their benefits. Although the benefits of optimising energy use can be demonstrated, the sharing of this data with other parties or combination with other lifestyle information to optimise at a more global level or provide new services, is still not clear.

Risk of Disruption: Increased interconnectivity between systems leads to increased vulnerability to cyber-attack. Security is a key concern and smarter grids lead to increased vulnerabilities from intrusions, error-caused disruptions, malicious attacks, destruction, and other threats. As the energy grid network is key to the operation of a country, there is naturally caution when it comes to the introduction of more smart technologies.

8.4 Barriers for Large and Small Companies

It is clear that none of the technologies and services being considered will become a market reality unless driven by industry. It was very notable in the interviews that a number of large world-wide companies had strong ambitions to gain market share in the key areas of Smart Cities, Smart Transportation and Smart Grid. These large companies already had strong European and US bases (generally through acquisition of local companies on both continents). It was thus easier for them to manage the existing differences in standards and requirements markets. There were, however, many smaller companies who also expressed an interest in gaining access to European and US markets, however, here there were some clear cultural issues that needed addressing.

In order to sell in the US it is necessary to be a US Corporate to be accepted. It is also impossible as a foreign company to sell to the US government. Breaking through this barrier by setting up a US corporate is challenging as a key indicator in the US is Gartner’s assessment of the company. This is more demanding for European companies new to the US as the key criteria is footprint in the US. There is also a cultural difference in doing business and another key issue not appreciated by European companies is that the marketing and sales pack is far more important in the US.

At the SME level there are also some fundamental differences in approaches to staffing and financing. In the US 5-10 MEuros is needed to start a company whereas it is far cheaper to set up and operate a company in the EU. The reason for this difference in financing is that more people are required in the US to create a start-up company as there is a cultural gap in the ways skills are used. It is common in the EU for engineers to be able to do multiple tasks and it is easy to find “swiss army knife” engineers in Europe. In the US people expect to work in one role and in general specialise in a specific function which each has its own manager. Although this looks like a disadvantage for US companies, by having people with separate roles it is easier to scale a business rapidly and grow as it is possible to replicate people with given skills.

9 Concluding Remarks

In total the report identifies 101 potential recommendations for EU-US collaboration from analysis of the current research activities and from interviews with industry. Additionally, further recommendations have also been collected from key PPPs, ETPs etc. and also the PICASSO Expert Groups. The recommendations are wide ranging and cover both general needs in terms of policy and standards, and also very specific technology needs. These recommendations will be assessed by the Expert Groups in the next phase of the PICASSO work and will be refined down into key recommendations for EU-US collaboration.

The analysis of existing programmes highlighted good correlation with the findings of interview with industry. It is clear that there are many opportunities for joint collaborations between the EU and US. The analysis of existing programmes identified a total 15 areas where it may be possible to collaborate on research and policy, 16 areas where there is an opportunity to work together on regulations and 9 areas where it would be beneficial to work together on standards.

In total the industry interviews highlighted 61 recommendations. Some of these were very specific and also linked with industry priorities, e.g. Industrial Internet Consortium, Industrie 4.0 and OPC-UA. There were, however, some common themes put forward by different industrial sectors in terms of the needs for standards for interoperability of interconnects, wireless communications, protocols and for data exchange. An overriding message was one of the need for data governance, clarity on data ownership and regulation for privacy and the strong need for security. An interesting new area that was highlighted was the shortage of skills and the need to provide proper education for future smart jobs. Here the need for agreement on appropriate accreditations was highlighted to avoid difficulties in movement of personnel or in enabling them to work on world-wide products.

Considering the societal domains the interviews highlighted that Smart Transportation was the most fertile area with a total of 12 recommendations for collaboration, with Smart Cities being the next most fertile area with 6 areas identified. The area of IoT/CPS is covered by a number of sectors represented notably the Chemical, Automation, Diagnostics, and Information Technology industries plus representation also from other sectors. The area of wireless telecommunications was also a fertile area with 6 areas being identified.

The opinions from ICT PPPs, ETPs, etc. were also sought. This included SmartGrids, ENIAC, ECSEL (ARTEMIS-IA, EPoSS and Aeneas were all individually contacted), NESSI, ETP4HPC, Big Data PPP, NEM, Networld2020, ALICE, ACARE, ERRAC, ERTRAC, Waterborne, KIC EIT, EFFRA and AIOTI. This highlighted that bodies representing the application domains that are constrained by commercial competition and regulations, e.g. aerospace, maritime, rail, etc. were less able to identify the potential for collaboration. Here there is still opportunity for fundamental work that addresses problems that are common across a number of stakeholders. PPPs and organisations addressing fundamental technologies, e.g. 5G, HPC, IoT and Big Data, highlighted a keenness to collaborate particularly in areas being addressed by their respective strategic research agendas.

The questionnaire was also circulated to the expert group members and their considered feedback was also collected. This highlighted a number of recommendations specific to the technology domains and also horizontal issues with respect to policy such as data privacy and security.

In summary the report identifies many areas where it would be possible for the EU and US to work together. There are key opportunities in the areas of Smart Cities and IoT/CPS which are rapidly developing areas and where there are common research, regulatory and standardisation needs. There are also great opportunities in the areas of Smart Energy and Smart Transportation, however, here there is existing regulation and legislation which needs to be harmonised. In the societal domains a number of more pragamatic barriers were also identificed which need to be addressed. Key barriers include a need for demonstration at scale, the funding and political will to support this, and the needs for public acceptance which requires trust in data privacy and security.

For the underlying technologies which are the basic building blocks of future applications, e.g. 5G, Big Data and IoT/CPS, there are many opportuntiies to work together. From a commericial perspective it is necessary to consider key areas where it is possible to collaborate at a pre-competitive level which would in future allow bilateral access to EU and US markets and would allow technology and products to be sold on the world stage increasing the competitiveness of EU and US companies in existing and developing markets.

10 References

[1] H. Thompson and D. Ramos-Hernandez, "Panorama of ICT landscape in EU and US: ICT, Policies, regulations, programmes and networks in the EU and US", 2016. http://www.picasso-project.eu/2016/10/12/interested-in-us-and-eu-landscape/

[2] European–United States Transportation Research Collaboration Challenges and Opportunities Report, February 2009.

[3] http://ec.europa.eu/programmes/horizon2020/en/h2020-section/high-performance-computing-hpc

[4] https://ec.europa.eu/digital-single-market/en/high-performance-computing]

[5] http://www.etp4hpc.eu/en/sra.html

[6] www.etp-alice.eu

[7] http://physicalinternetinitiative.org/

[8] World Bank (2016): DIGITAL DIVIDENDS, World development report 2016: http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2016/01/13/090224b08405ea05/2_0/Rendered/PDF/World0developm0000digital0dividends.pdf

[9] ALICE Recommendations to H2020 Work Programs 2016-2017, December 2014: http://www.etp-logistics.eu/wp-content/uploads/2015/07/ALICE-Recomendations-HORIZON2020-WP-2016-2017-v141218_DEF-2.pdf

[10] European Technology Platform on Logistics input for the first calls of the HORIZON 2020: http://www.etp-logistics.eu/wp-content/uploads/2015/08/European-Technology-Platform-on-Logistics-input-for-the-first-calls-of-the-HORIZON-2020.pdf